日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　２００３年　６月　２日

出　願　番　号
Application Number:　特願２００３－１５６１２７

[ST. 10/C]:　[ＪＰ２００３－１５６１２７]

出　願　人
Applicant(s):　株式会社日立製作所

２００３年　８月２６日

特許庁長官
Commissioner,
Japan Patent Office　今井康夫

出証番号　出証特２００３－３０６９６４３

【書類名】　特許願

【整理番号】　H03001281A

【あて先】　特許庁長官　殿

【国際特許分類】　G06F 12/00

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

【氏名】　橋本　顕義

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【電話番号】　03-3212-1111

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　ファイルサーバシステム

【特許請求の範囲】

【請求項１】

ネットワークを介して複数のクライアントと接続された複数の磁気ディスク駆動装置と、

該ネットワークに接続され、前記クライアントから前記磁気ディスク駆動装置へのアクセス要求を受け付け、前記複数の磁気ディスク駆動装置のデータ入出力を管理するファイル制御部を備えたファイルサーバシステムであって、

前記ファイル制御部は前記複数の磁気ディスク駆動装置の各々を特定できる複数のＩＤ情報を登録可能な構成情報を有し、

さらに、前記ファイル制御部は前記ネットワークを介して磁気ディスク駆動探索メッセージをブロードキャストし、

該磁気ディスク駆動探索メッセージを受信した前記磁気ディスク駆動装置は、自磁気ディスク駆動装置を特定できる前記ＩＤ情報を前記ファイル制御部に返信し、

前記返信されたＩＤ情報を受信した前記ファイル制御部は、前記ＩＤ情報を返信した磁気ディスク駆動装置に対して、該ファイル制御部以外の前記ネットワークに接続された機器との通信を制限するように設定することを特徴とするファイルサーバシステム。

【請求項２】

請求項１記載のファイルサーバシステムであって、

前記ファイル制御部に接続された、保守作業を行うための管理端末をさらに備えたことを特徴とするファイルサーバシステム。

【請求項３】

請求項２記載のファイルサーバシステムであって、

前記ファイル制御部と前記磁気ディスク駆動装置との間に接続され、前記管理端末と前記磁気ディスク駆動装置との通信を制御可能であるファイアウォールを備えたことを特徴とするファイルサーバシステム。

【請求項４】

請求項２記載のファイルサーバシステムであって、

前記ファイル制御部は、前記管理端末との通信を、前記クライアントとの通信および前記磁気ディスク駆動装置との通信よりも優先して行うことを特徴とするファイルサーバシステム。

【請求項５】

請求項１記載のファイルサーバシステムであって、

前記ファイル制御部および前記複数の磁気ディスク駆動装置はiSCSIインターフェースを備え、前記ネットワーク上でIPプロトコルを用いて通信することを特徴とするファイルサーバシステム。

【請求項６】

請求項１記載のファイルサーバシステムであって、前記磁気ディスク駆動装置は、該磁気ディスク駆動装置に対して前記ネットワークを介して通信の許可を求めてきた前記ネットワークに接続した機器との通信の許可、不許可を判定することを特徴とするファイルサーバシステム。

【請求項７】

請求項６記載のファイルサーバシステムであって、前記磁気ディスク駆動装置は、前記ネットワークに接続した機器の一部または全部のネットワーク上の識別子と、

前記識別子に対応する前記機器の認証コードを登録可能な認証情報を有し、

さらに該磁気ディスク駆動装置は、前記ネットワーク上のいずれかの機器が通信の許可を求めてきた場合に、前記機器が送信する認証コードと前記認証情報内に登録した認証コードを比較し、これら2つの認証コードが一致すれば通信を許可し、一致しなければ通信を許可しないことを特徴とするファイルサーバシステム。

【請求項８】

請求項７記載のファイルサーバシステムであって、前記磁気ディスク駆動装置は、ネットワーク経由で受信した前記認証情報の変更命令に従って前記認証情報を変更することを特徴とするファイルサーバシステム。

【請求項９】

請求項８記載のファイルサーバシステムであって、システム起動時に前記ファイル制御部が前記磁気ディスク駆動装置に対して前記認証情報の変更命令を発行し、前記磁気ディスク駆動装置が前記ファイル制御部以外の機器との通信を禁止する設定を行うことを特徴とするファイルサーバシステム。

【請求項１０】

請求項１記載のファイルサーバシステムであって、前記ファイル制御部は、該ファイルサーバシステムの管理者が前記ファイル制御部と前記クライアントの間の通信で送受信されるデータ量と、前記ファイル制御部と前記磁気ディスク駆動装置の間の通信で送受信されるデータ量の比率を設定する手段を有し、

前記ファイル制御部と前記クライアントの間の通信で送受信されたデータ量と、前記ファイル制御部と前記磁気ディスク駆動装置の間の通信で送受信されたデータ量とを計測し、データ量の計測値の比率が前記設定された比率に近づくように通信処理の優先度を制御することを特徴とするファイルサーバシステム。

【請求項１１】

互いに接続して１つのネットワークを形成する複数のスイッチングハブと、

該ネットワークを介してクライアントと接続された複数の磁気ディスク駆動装置及び

ファイル制御部を備え、

前記複数の磁気ディスク駆動装置はそれぞれ前記複数のスイッチングハブのうちの1つと接続し、

前記ファイル制御部は前記複数のスイッチングハブのうちの1つと接続し、

前記ファイル制御部は、前記クライアントから受けた前記磁気ディスク駆動装置へのアクセス要求を受け付け、前記複数の磁気ディスク駆動装置のデータ入出力を管理するファイルサーバシステムであって、

前記スイッチングハブは、

前記ファイル制御部と前記複数のクライアントが1つの仮想的なネットワークに属し、

前記ファイル制御部と前記複数の磁気ディスク駆動装置がもう1つの仮想的なネ

ットワークに属するように制御することを特徴とするファイルサーバシステム。

【請求項１２】

請求項１１記載のファイルサーバシステムであって、前記複数のスイッチングハブの1つに接続し、前記ファイル制御部の保守作業を行うための管理端末をさらに備えたことを特徴とするファイルサーバシステム。

【請求項１３】

請求項１２記載のファイルサーバシステムであって、前記スイッチングハブは、

前記ファイル制御部と前記複数のクライアントが1つの仮想的なネットワークに属し、

前記ファイル制御部と前記複数の磁気ディスク駆動装置がもう1つの仮想的なネットワークに属し、

前記ファイル制御部と前記管理端末は前記2つとは異なる第3の仮想的なネットワークに属するように制御することを特徴とするファイルサーバシステム。

【請求項１４】

請求項１３記載のファイルサーバシステムであって、前記仮想的なネットワークはVLAN(Virtual LAN)であることを特徴とするファイルサーバシステム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、計算機システム、特にネットワークを介して結合した複数のクライアントにファイルサービスを提供するファイルサーバに関する。

【０００２】

【従来の技術】

ネットワークで結合した複数の計算機間でデータを共有する技術は１９８０年代から開発されていた。データ共有技術でもっとも普及した技術としては、Sun Microsystems社のNFS(Network File System)がある。NFSに関しては、非特許文献１に簡単な解説が記載されている。NFSは、データをファイル単位で管理する技術である。ファイルを保存する計算機をファイルサーバ、ファイルサーバ

が保存したファイルをネットワーク経由で利用する計算機をクライアントという。NFSは、ファイルサーバが保存したファイルをあたかもクライアントのディスク内に保存されているようにユーザにみせる技術である。実際には、NFSはファイルサーバとクライアント間のネットワーク通信プロトコルとして定義される。

【０００３】

近年、ネットワークコンピューティングの急速な普及に伴い、LANのようなIPネットワークに直接接続できる二次記憶装置に関する技術が提案されている。たとえば、NetSCSI、NASD(Network Attached Secure Disks)やIETF(Internet Engineering Task Force)で規格が制定されたiSCSI規格がその例である。NetSCSI、NASDに関しては、非特許文献２に詳しい。iSCSIはIPネットワーク上SCSI(Small Computer System Interface)プロトコルの通信を可能とする規格であり、その詳細は、非特許文献３に詳しい。

【０００４】

NetSCSIやNASDに共通のの構成を図2に示す。図2のシステムでは、ファイルサービスを受けるクライアント(101)と、データを保存する磁気ディスク駆動装置(103)と、磁気ディスク駆動装置(103)を管理、制御するファイル制御部(105)がLAN(100)に結合した形態をとる。磁気ディスク駆動装置(103)は、データを記録する磁気ディスク媒体(106)、LAN(100)に結合した機器と通信を行い、他の機器からの命令に従って前記磁気ディスク媒体(106)にデータを記録するディスク制御部(107)からなる。ディスク制御部(107)は、通常のデータのリード、ライト制御機能以外に、LAN(100)に接続した他の機器との通信を許可、不許可を判定する認証制御部(108)を持ち、認証制御部(108)は通信を許可された機器の情報を記録する認証情報(109)を持つ。ファイル制御部(105)は、LAN上の通信を行うLANコントローラ(114)、磁気ディスク駆動装置(103)上のデータをファイルとしてクライアント(101)に提供するファイルシステム、磁気ディスク駆動装置(103)のアクセス権限を制御するアクセス制御部(116)からなる。非特許文献２によれば、図2のシステムの動作は、おおむね以下のようになる。

クライアント(101)がファイル制御部(105)にファイルアクセスのための命令を送信する。ファイルアクセス命令を受信したファイル制御部(105)は、ファイルシ

ステム(115)がクライアント(101)の要求を解析し、要求されたデータを保存する磁気ディスク駆動装置(103)に対してデータ入出力命令を発行する。入出力命令を受信した磁気ディスク駆動装置(103)は、前記ファイルアクセス命令を発行したクライアント(101)との間でデータ転送を行う。データ転送が完了すると、磁気ディスク駆動装置(103)は、データ転送完了をファイル制御部(105)に報告する。データ転送完了の報告を受けたファイル制御部(105)は、クライアント(101)に当該ファイルアクセス命令の完了を報告する。

【０００５】

また、磁気ディスク駆動装置(103)は、クライアント(101)と通信を行う。したがって、クライアントを認証するための認証制御部(108)を持つ。ファイル制御部(105)は、これら磁気ディスク駆動装置(103)のセキュリティポリシを決定するアクセス制御部(116)を持つ。

また、非特許文献２では、ファイル制御部(105)と磁気ディスク駆動装置(103)間の通信を暗号化し、仮想的な通信チャネルを生成することも開示されている。このことにより、クライアント(101)は、ファイル制御部(105)と磁気ディスク駆動装置(103)間の通信を盗み見ることができなくなる。

さらに、ファイルサーバ装置は、ディスプレイやキーボードを持たず、ユーザがLAN(100)に接続した管理端末よりファイルサーバ装置の操作を行うのが通例である。

【非特許文献１】

「最前線　UNIX（登録商標）のカーネル」(ユーレッシュ・バファリア著　徳田　英幸、中村　明、戸辺　義人、津田　悦幸訳　株式会社ピアソン・エデュケーション　2000)

【非特許文献２】

「File Server Scaling with Network-Attached Secure Disks」(Garth A. Gibson他著、論文誌"THE 1997 ACM SIGMETRICS INTERNATIONAL CONFERENCE ON MEASUREMENT AND MODELING OF COMPUTER SYSTEMS"、272-284ページ)

【非特許文献３】

「Internet　Draft　iSCSI」(Julian　Satran他著　2002)

【０００６】

【発明が解決しようとする課題】

本発明の第1の課題は、クライアントと磁気ディスク駆動装置が同一LANに結合した場合に、磁気ディスク駆動装置内に保存されたデータの安全性を確保することにある。非特許文献２に記載された従来技術は、クライアント(101)と磁気ディスク駆動装置(103)がデータの送受信を行うことを特徴としており、クライアント(101)が磁気ディスク駆動装置(103)のデータを直接読み取ることが可能である。この方法では、クライアント(101)が前述の手順を守る限りデータの安全性を保つことができるが、クライアント(101)はファイル制御部(105)にファイルアクセス要求を送信することなく、直接磁気ディスク駆動装置(103)のデータにアクセスすることも可能である。そもそも、磁気ディスク駆動装置(103)がクライアント(101)との通信を許可しているため、前述のようなファイル制御部(105)の許可のないアクセスを磁気ディスク駆動装置(103)が防ぐことはできない。

【０００７】

本発明第2の課題は、ファイル制御部(105)とディスク駆動装置(103)の間の通信を暗号化するときの処理量の問題である。非特許文献２に記載された従来技術では、ファイル制御部(105)とディスク駆動装置(103)の間の通信を暗号化通信でおこなう。これは、ファイル制御部(105)とディスク駆動装置(103)の間の通信データをクライアント(101)が取得することを防ぐためである。通常、送受信されるデータを暗号化、復号化する処理は多大な計算量が必要とする。個々の磁気ディスク駆動装置に実用的な通信速度を実現できる暗号化、復号化処理機能を搭載することは現状ではコスト上昇を招く。

【０００８】

本発明第3の課題は、LAN(100)上を性質の異なる複数のトラフックが流れることにより、それぞれのトラフィックを適切に処理できないという課題である。すなわち、磁気ディスク駆動装置(103)に対するデータ入出力のトラフィックは、データ転送量が多い。一方、クライアント(101)とファイル制御部(105)の通信トラフィックや、管理端末とファイル制御部(105)の通信トラフィックは比較的データサイズが小さい。仮に保守員が管理端末よりファイル制御部(105)を操作し

ようとしたときに、ファイル制御部(105)が大量のデータ転送を行っていた場合、操作に遅延が発生する。この遅延が甚だしい場合、ファイル制御部(105)が操作不能となる。

【０００９】

【課題を解決するための手段】

前記第1の課題を解決するため、磁気ディスク駆動装置に初めて電源を投入したときなどに、ファイル制御部が磁気ディスク駆動装置に対して、前記ファイル制御部以外の機器との通信を制限するように設定することを許容する。本手段によって、クライアントや管理端末がファイル制御部の許可なく磁気ディスク駆動装置のデータを読み取る、または書き込むことを防ぐことができ、データの安全性を確保することができる。その結果、データは必ずファイル制御部を経由することになる。

【００１０】

前記第2の課題を解決するため、VLAN(Virtual　LAN)を導入する。VLANとは、物理的なネットワーク上に仮想的なネットワークを構築し、構成変更が容易なネットワークシステムを実現する方法であり、LANを構成するスイッチやルータによって実現される。VLAN技術については、「VPN/VLAN教科書」(是友　春樹監修、マルチメディア通信研究会編、アスキー出版局、1999)に詳しい。このVLANをファイルサーバに適用すれば前記第2の課題を解決することができる。すなわち、ファイル制御部とクライアントを同一VLANに所属させる。またファイル制御部と磁気ディスク駆動装置を前記VLANとは別の第2のVLANに所属させる。最後に、ファイル制御部と管理端末を第3のVLANに所属させる。異なるVLAN間では通信は不可能なので、クライアント、管理端末が磁気ディスク駆動装置に直接アクセスすることを禁止できる。これは、LANを構成するスイッチやルータによって実現されるため、ファイル制御部や磁気ディスク駆動装置に暗号化通信機能を搭載する必要はなく、コスト低減につながる。

【００１１】

前記第3の課題を解決するため、ファイル制御部がLAN通信処理の優先度を、通信相手ごとに設定することを許容する。すなわち、管理端末との通信を最優先に

処理するように設定できれば、管理端末からファイル制御部を常に操作可能となる。このような優先度制御は、別の面でも有効である。一般のサーバに対して過大なネットワーク負荷をかけることでサービスを停止させる攻撃方法が知られている。ファイル制御部がこのような攻撃を受けた場合でも、本発明の優先制御を用いれば管理端末から操作可能であり、ファイルサービスを停止させることはない。

【００１２】

【発明の実施の形態】

以下、図面を用いて本発明の実施の形態を説明する。

<実施例1>

図1に本発明のファイルサーバの構成図を示す。ファイルサービスを受けるクライアント(101)と、データを保存する磁気ディスク駆動装置(103)と、前記磁気ディスク駆動装置(103)のデータ入出力を管理し、前記クライアント(101)に対してファイルサービスを提供するファイル制御部(105)がLAN(100)に結合している。本実施例では、LAN(100)はIEEE802.3規格で規定されたLAN(一般にはイーサネット（登録商標）と呼称される)を想定しているが、本発明がLAN(100)の種類に依存しないことはいうまでもない。またLAN(100)上の通信にはTCP/IPプロトコルで通信することを想定している。本発明は、TCP/IPプロトコルに依存しないこともいうまでもない。

【００１３】

磁気ディスク駆動装置(103)は、磁気ディスク媒体(106)と磁気ディスク制御部(107)からなる。磁気ディスク制御部(107)は磁気ディスク媒体(106)に対する入出力を行う以外に、LAN(100)経由の通信の許可/不許可を決定する認証制御部(108)と認証情報(109)を有する。認証情報(109)には、磁気ディスク駆動装置(103)とLAN(100)経由で通信を行うことを許可されたネットワーク機器に関する情報が記録されている。認証制御部(108)は、LAN(100)に接続されたネットワーク機器が磁気ディスク駆動装置(103)に対して通信の許可を求めてきたときに、認証情報(109)を参照し、通信の許可、不許可を決定する。すなわち、認証情報(109)に登録されていないネットワーク機器から通信の許可を求められたとき、認証制御

部(108)は、通信の不許可を当該ネットワーク機器に応答する。また、利用者、管理者からの命令に従って、認証制御部(108)は、認証情報(109)の変更も行う。

【００１４】

ファイル制御部(105)は、LAN制御部(114)、ファイルシステム(115)、アクセス制御部(116)、構成情報(117)、優先度制御部(118)から構成される。ファイルシステム(115)は、磁気ディスク駆動装置(103)の記録領域を管理し、これら記憶領域をクライアント(101)に対してファイルとして仮想的に実現する機能である。LAN制御部(114)は、ファイル制御部(105)がLAN(100)を用いて通信を行うための機能である。構成情報(117)は、磁気ディスク駆動装置(103)の種類、個数などの装置構成に関する情報である。アクセス制御部(116)は、磁気ディスク駆動装置(103)のセキュリティ設定を行う。優先度制御部(118)は、ファイル制御部(105)が行うLAN(100)上の通信において、優先度を指定し、その優先度に従って通信することを実現する。本実施例では、ファイル制御部(105)が磁気ディスク駆動装置(103)に対してデータ入出力を行うが、そのプロトコル規格として、iSCSIを使う、つまり、ファイル制御部(105)及び磁気ディスク駆動装置(103)がiSCSIインターフェースを有するという前提で説明する。しかし、本発明は、iSCSIに依存しないことはいうまでもない。

【００１５】

次に図3を使って構成情報(117)を説明する。構成情報(117)は、ファイル制御部(105)がデータを保存するために使用する磁気ディスク駆動装置(103)に関するID情報等の情報を保存する。番号(300)は、ファイル制御部(105)が磁気ディスク駆動装置(103)に対して内部的に付与する番号である。MACアドレス欄(301)は、磁気ディスク駆動装置(103)のMACアドレスを示す。MACアドレスとは、IEEE802.3規格により規定されたネットワーク機器固有の番号である。MACアドレスは、個々のネットワーク機器に製造段階で付与される。磁気ディスク駆動装置(103)はLAN(100)に直接結合できるため、MACアドレスを持っている。ファイル制御部(105)は、磁気ディスク駆動装置(103)のMACアドレスを取得して構成情報(117)のMACアドレス欄(301)に登録する。IPアドレス欄(302)は、磁気ディスク駆動装置(103)のIPアドレスが登録される。磁気ディスク駆動装置(103)に対するIPアドレスの

設定方法であるが、利用者がなんらかの治具で設定する方法、DHCP(Dynamic Host Configuration Protocol)を用いて磁気ディスク駆動装置(103)が自動的にIPアドレスを設定する方法など、さまざまある。本実施例では、磁気ディスク駆動装置(103)がなんらかの方法でIPアドレスの取得に成功したものとして説明する。HDD識別子欄(303)は、磁気ディスク駆動装置(103)固有の識別子を登録する欄である。この識別子は、MACアドレスとも異なる。すなわち、ルータを介した通信の場合には、MACアドレスは識別子とならず、ネットワークに接続された機器の固有の識別子とならないからである。LANの規格では、情報を送信するネットワーク機器は、送信する情報に付随してMACアドレスを通信相手に送信する。そのため、受信側ネットワーク機器は、送信元のネットワーク機器を識別することができる。一方、送信側ネットワーク機器と受信側ネットワーク機器が異なるネットワークにある場合は、状況が異なる。この場合、送信側ネットワーク機器が送信した情報とMACアドレスは一旦ルータが受信する。そしてルータが受信側に情報を送信する。このとき、ルータはMACアドレスをルータ自身のMACアドレスに変更して送信する。そのため、送信側ネットワーク機器と受信側ネットワーク機器がルータを介して通信する場合には、MACアドレスはネットワーク機器固有の識別子となりえない。そのため、iSCSI規格では、iSCSIプロトコルで通信可能なネットワーク機器に固有の識別子を付与する仕様が提案されている。複数の識別子が記載されているが、本実施例ではEUIという64bitの識別子を用いて説明する。EUIについては、非特許文献３に詳しい。HDD識別子欄(303)には、EUIが16進法で登録されている。Alias名欄(304)は、磁気ディスク駆動装置(103)のEUIによる識別子とは別名が登録される。EUIはネットワーク機器を識別することは可能だが、利用者にはそのEUIを持つネットワーク機器がどのような機器か判別しにくい。そのため、利用者にわかりやすい形式の別名をAlias名欄(304)に登録する。図3のAlias名は、「Hitachi-OPEN-K-sn-XXXXXXX」という形式になっている。「Hitachi」がベンダ名、「OPEN-K」が製品型名、「sn」は以下に続く数字が製造番号を示し、「XXXXXXX」が製造番号である。このAlias名により利用者はネットワーク機器の型名などを把握できるようになる。Alias名は、識別子ではないので、ネットワーク機器に固有の番号となっている必要はない。また、Alias名は本実

施例ではその一例を示したに過ぎず、本発明はAlias名の形式に依存しないことはいうまでもない。構成情報(117)に登録される磁気ディスク駆動装置(103)の情報のうち、HDD識別子は、管理者によってあらかじめ設定される。これは、管理者が、ファイル制御部(105)が利用できる磁気ディスク駆動装置をあらかじめ指定しておくことで、他のファイル制御部が使用中の磁気ディスク駆動装置にデータを書きこんで、データ破壊を起こすことができないようにすることができる。

【００１６】

次に図4、5に磁気ディスク装置(103)の認証情報(109)を示す。図4が認証情報(109)の初期状態を示し、図5がファイル制御部(105)によって情報を設定された後の状態を示す。図4、5の1つの行が磁気ディスク駆動装置(103)が通信を許すネットワーク機器の情報を示す。MACアドレス欄(400)、(500)は、磁気ディスク駆動装置(103)が通信を許すネットワーク機器のMACアドレスを登録する欄である。IPアドレス欄(401)、(501)は、磁気ディスク駆動装置(103)が通信を許すネットワーク機器のIPアドレスを登録する欄である。認証コード欄(402)、(502)は、通信の許可、不許可を判定するための認証コードを登録する欄である。オーナフラグ(403)、(503)は、認証情報(109)に登録されたネットワーク機器の中で、磁気ディスク駆動装置(103)の所有者を示すフラグである。本実施例では、オーナフラグ(403)が「1」のとき当該ネットワーク機器が磁気ディスク装置(103)の所有者とする。オーナフラグ(404)が「1」でないとき、当該ネットワーク機器は磁気ディスク駆動装置(103)の所有者ではない。そして、認証情報(109)は、磁気ディスク駆動装置(103)の所有者でなければ変更できない。

【００１７】

ネットワーク機器は、磁気ディスク駆動装置(103)と通信を開始するときに、磁気ディスク駆動装置(103)に対して通信の許可を求めるため、磁気ディスク駆動装置(103)に認証コードを送信する。磁気ディスク駆動装置(103)は、この送信された認証コードと登録された認証コードを比較し、一致すれば、通信を許可し、一致しなければ通信を許可しない。本実施例では、以上に述べた方法で認証するが、認証の方法は多数知られている。本発明は認証の方法に依存しないことは言うまでもない。磁気ディスク駆動装置(103)は、認証情報(109)のLAN(100)経由

の変更を許す点を特徴としているが、MACアドレス欄(404)は、「Every one」となっている。これは、すべてのネットワーク機器に対して通信を許可することを示す。必ずしも「Every one」という文字列ではなく、すべてのネットワーク機器に対して通信を許可することを示す符号であればよい。本実施例では、この符号として「Every one」を用いることにする。磁気ディスク駆動装置(103)の初期状態では、すべてのネットワーク機器に対して通信を許可する状態になっている。IPアドレス欄(405)も「Every one」となっており、すべてのネットワーク機器に対して通信を許可する状態になっている。認証コード欄(406)は、「00000000_00000000_00000000_00000000」となっている。これは認証コードが設定されていない状態になっている。図5では、ファイル制御部(105)が認証情報(109)に情報を設定した後の状態を示している。図5では、MACアドレス欄(504)、IPアドレス欄(505)、認証コード欄(506)に値が設定されている。磁気ディスク駆動装置(103)は、認証情報(109)に記載されたネットワーク機器とのみ通信を行う。そして、認証情報の行を増やすことで、複数のネットワーク機器との通信を許可することも可能である。

【００１８】

認証情報(109)は、LAN(100)に接続したネットワーク機器から変更可能である点に特徴がある。通常、このような認証情報は利用者あるいは管理者が、磁気ディスク駆動装置(103)がLAN(100)に接続される前に、LAN(100)以外の手段で設定するのが通例である。なぜなら、このような認証コードはLAN(100)以外の安全な経路で設定しなければ意味がないからである。磁気ディスク駆動装置(103)のような装置では、認証情報(109)はEEPROMや、フラッシュメモリのような不揮発メモリに格納されることが多く、認証情報(109)の書き換えは専用の治具で行う。ところで、現代のファイルサーバの中には大量の磁気ディスク駆動装置(103)を搭載するシステムも少なくない。このようなシステムでは、1台1台の磁気ディスク駆動装置に専用の治具で認証情報を設定するのは、非常に煩雑であり、現実的でない。従って、ファイル制御部(105)がLAN(100)経由で認証情報(109)を設定する方法が、合理的である。なぜなら、ファイル制御部(105)により前記手順が自動化されるからである。しかし、認証情報(109)がLAN(100)経由で設定可能だと

、磁気ディスク駆動装置(103)と通信が許可されていないネットワーク機器でも認証情報(109)を変更し、磁気ディスク駆動装置(103)との通信が可能になってしまう。つまり、認証情報(109)が認証情報としての役割を果たさないことになる。そこで、オーナフラグ(403)が「1」であるネットワーク機器のみ認証情報(403)を変更可能とする。磁気ディスク駆動装置(103)を設置後、利用者が初めて磁気ディスク駆動装置(103)に電源を投入するときに、ファイル制御部(105)が自らの認証コードを設定するとともに、オーナフラグ(403)を「1」とする。この過程を図6に示す。

ステップ(600)　磁気ディスク駆動装置(103)に電源が投入されるステップ。

ステップ(601)　磁気ディスク駆動装置(103)がLAN(100)より認証情報(109)の変更命令を受信したか判定するステップ。受信していなければ、命令を待つか、他の処理を実行する。

ステップ(602)　磁気ディスク駆動装置(103)が認証情報(109)の変更命令を受信した場合、認証情報(109)を検査する。検査した結果、オーナフラグ欄(407)が「1」に設定されたエントリがあるか判断する。オーナフラグ欄(407)が「1」に設定されたエントリがあった場合、ステップ(603)に進む。オーナフラグ欄(407)に「1」が設定されたエントリがない場合、ステップ(607)に進む。

ステップ(603)　すでにオーナフラグ欄(407)に「1」が設定されたエントリがあった場合、所有者であるネットワーク機器のみが認証情報(109)の変更可能である。ステップ(603)では認証情報変更命令を発行したネットワーク機器が所有者かどうかを判定する。当該認証情報変更命令を発行したネットワーク機器が磁気ディスク駆動装置(103)の所有者であれば、ステップ(604)に進む。所有者でなければ、ステップ(606)に進む。

ステップ(604)　磁気ディスク駆動装置(103)の所有者が認証情報(109)を変更していることが確認できたので、当該命令に従い、磁気ディスク駆動装置(103)の認証制御部(108)が認証情報(109)を変更する。変更内容は、送信元が本認証情報変更命令とともに送信する。

ステップ(605)　磁気ディスク駆動装置(103)は認証情報変更命令を発行したネットワーク機器に変更の完了を報告する。

ステップ(606)　当該認証情報変更命令が磁気ディスク駆動装置(103)の所有者以外から送信された場合、磁気ディスク駆動装置(103)は認証情報変更命令の発行元に変更失敗を報告する。

ステップ(607)　所有者が設定されていない場合、どのネットワーク機器でも認証情報(109)を変更することができる。本ステップでは、本命令を送信したネットワーク機器の情報を設定する。

ステップ(608)　さらに、ステップ(607)で設定したネットワーク機器のエントリのオーナフラグ欄(407)に「1」を設定する。つまり、磁気ディスク駆動装置(103)に最初に認証情報変更命令を発行したネットワーク機器が磁気ディスク駆動装置(103)の所有者となるわけである。

ステップ(609)　処理の終了。

【００１９】

図7のラダーチャートを用いて図1のファイルサーバの初期化手順を説明する。時間軸(700)は、ファイル制御部(105)の時間軸を示し、時間軸(701)は磁気ディスク駆動装置(103)の時間軸を示す。

ステップ(702)　ファイル制御部(105)の電源投入のステップ。

ステップ(703)　磁気ディスク駆動装置(103)の電源投入ステップ

ステップ(704)　ファイル制御部(105)に搭載され、ファイルサービスを実現するファイルシステム(115)が起動するステップ。

ステップ(705)　磁気ディスク駆動装置(103)が起動し、ネットワーク設定を行うステップ。前述のDHCPなどの方法でIPアドレスを取得するステップを含む。

ステップ(706)　ファイル制御部(105)がLAN(100)に接続された磁気ディスク駆動装置(103)を探索するディスカバリメッセージ（磁気ディスク駆動探索メッセージ）を発信する。ファイル制御部(105)はディスカバリメッセージをブロードキャストで発信する。これらディスカバリ手順については、「iSCSI Naming and Discovery」(Mark Bakkek他著 2003年)(以下文献1)に詳しい。

ステップ(707)　磁気ディスク駆動装置(103)はステップ(706)のディスカバリメッセージを受信する。

ステップ(708)　磁気ディスク駆動装置(103)はファイル制御部(105)にディスカ

バリメッセージに対する応答メッセージを送信する。応答メッセージの内容は、図3で説明した、MACアドレス、IPアドレス、HDD識別子、Alias名などである。

ステップ(709)　磁気ディスク駆動装置(103)の応答メッセージを受信する。

ステップ(710)　応答メッセージには、HDD識別子が含まれているので、ファイル制御部(105)は図3の構成情報(117)にあらかじめ登録されているHDD識別子と照合する。登録は、本ファイルサーバの管理者が行う。応答メッセージのHDD識別子と構成情報(117)にあらかじめ登録されたHDD識別子が一致していれば、ファイル制御部(105)は、MACアドレス、IPアドレス、Alias名を構成情報(117)に登録していく。ファイル制御部(105)は、すべての応答メッセージに対して、照合作業を続ける。そして、ファイル制御部(105)は、あらかじめ構成情報(117)に登録された磁気ディスク駆動装置(103)から応答メッセージを受信したことを確認する。構成情報(117)に登録された磁気ディスク駆動装置(103)の中で、1つでも応答メッセージを送信しなかった磁気ディスク駆動装置(103)があった場合には、ファイル制御部(105)は、管理端末にエラーを表示して初期化を中断する。ファイル制御部(105)が構成情報(117)に登録された磁気ディスク駆動装置(103)すべてから応答メッセージを受信したことを確認した場合には、そのまま初期化手順を続行する。

ステップ(711)　ファイル制御部(105)が磁気ディスク駆動装置(103)に対して、認証情報(109)を変更するメッセージを送信する。前述の通り、磁気ディスク駆動装置(103)は初期状態では、どのネットワーク機器からも通信可能な状態となっているため、通信を許可するネットワーク機器としてファイル制御部(105)のみを指定するものとする。具体的には、図5の認証情報(117)にファイル制御部(105)のMACアドレス、IPアドレス、認証コードを設定し、他のネットワーク機器の認証情報は設定しない。磁気ディスク駆動装置(103)は、図6の手順に従って認証情報(109)を変更する。

ステップ(712)　ファイル制御部(105)が送信した認証情報設定メッセージを、磁気ディスク駆動装置(103)が受信する。

ステップ(713)　ステップ(712)で受信したメッセージに従って磁気ディスク駆動装置(103)が認証情報(109)に情報を設定する。本ステップによって、ファイル制

御部(105)がデータを保存する磁気ディスク駆動装置(103)をクライアント(101)、管理端末がアクセスすることができなくなりデータの保全が可能になる。図6の手順に従えば、オーナフラグ(403)も「1」に設定される。すでに他のネットワーク機器が、磁気ディスク駆動装置(103)の認証情報(109)に自機器の認証情報を設定した場合、ファイル制御部(105)は自らの認証情報(109)を設定できない。

ステップ(714)　認証情報(109)の変更が終了すると、磁気ディスク駆動装置(103)は認証情報設定の完了をファイル制御部(105)に報告する。すでに他のネットワーク機器が、磁気ディスク駆動装置(103)の認証情報(109)に自らの認証情報を設定した場合は、磁気ディスク駆動装置(103)は認証情報(109)の設定が失敗したことをファイル制御部(105)に報告する。

ステップ(715)　ステップ(713)で磁気ディスク駆動装置(103)が送信した報告をファイル制御部(105)が受信する。ファイル制御部105)は、認証情報(109)に自らの情報を設定できなかった場合には、管理端末にその情報を表示し管理者に報告する。

ステップ(716)　ファイル制御部(105)が磁気ディスク駆動装置(103)に対して通信の許可を求めるステップである。この手続きをログインといい、文献1にその一例が記載されている。本ステップにて、ファイル制御部(105)は認証コードを送信する。

ステップ(717)　ステップ(716)でファイル制御部(105)が送信した認証コードを磁気ディスク駆動装置(103)が受信する。

ステップ(718)　磁気ディスク駆動装置(103)は受信した認証コードが認証情報(109)に登録されているか判定する。

ステップ(719)　認証コードが認証情報(109)に登録されていれば、磁気ディスク駆動装置(103)にログイン受諾メッセージを送信する。認証コードが認証情報(109)に登録されていなければ、ログイン拒絶メッセージを送信する。

ステップ(720)　ファイル制御部(105)は磁気ディスク駆動装置(103)が送信したログイン受諾または拒絶メッセージを受信する。

ステップ(721)　ファイル制御部は(105)は、磁気ディスク駆動装置(103)がログインを受諾した場合には、そのまま磁気ディスク駆動装置(103)にアクセスでき

る。

次に図8、9、10を用いて、クライアント(101)が磁気ディスク駆動装置(103)に保存されているファイルを読み込んだり、書き込んだりする動作を説明する。図8は、クライアント(101)がファイルを読み込む動作を示したラダーチャートである。時間軸(800)がクライアント(101)の処理の流れ、時間軸(801)がファイル制御部(105)の処理の流れ、時間軸(802)が磁気ディスク駆動装置(103)の処理の流れである。

ステップ803 クライアント(101)がファイル制御部(105)にファイルリード要求を送信する。本実施例では、クライアント(101)とファイル制御部(105)の間の入出力プロトコルは前述のNFSを前提としている。NFSでは、リード要求は、ファイル名または、ファイルを一意に識別できる識別子と要求するデータのファイル先頭からのオフセット位置、要求するデータサイズなどを送信する。

ステップ804 ファイル制御部(105)が前記リード要求を受信する。

ステップ805 ファイルシステム(115)が受信した情報から、クライアント(101)が要求するデータが磁気ディスク駆動装置(103)のどこに保存されているか探索する。SCSI規格のような入出力プロトコルでは、磁気ディスク駆動装置(103)はある固定サイズの記憶領域(典型的には512B)の集合体として扱われる。前記固定サイズの記憶領域1つ1つには番号がつけられる。この番号をLBA(Logical Block Address)という。磁気ディスク駆動装置(103)にもそれぞれ番号がつけられており、LUN(Logical Unit Number)という。したがって、ファイル制御部(105)は、磁気ディスク駆動装置(103)内のデータにアクセスしたい場合には、LUN、LBA、要求データサイズを指定することになる。このように、ファイルシステム(115)の機能は、クライアント(101)からファイル名またはその識別子で指定された入出力命令をLUN、LBA、要求データサイズで指定される入出力命令に変換することと言える。

ステップ806 ファイルシステム(115)の処理によって、クライアント(101)が要求するデータの位置(LUN、LBA)が判明したところで、ファイル制御部(105)は、当該データを保存した磁気ディスク駆動装置(103)に読み込み命令を送信する。前述のように読み込み命令はLUN、LBA、データサイズを指定する形式をとる。

ステップ807　磁気ディスク駆動装置(103)がファイル制御部(105)が発行した読み込み命令を受信する。

ステップ808 磁気ディスク駆動装置(103)が前記読み込み命令に従って要求されたデータをファイル制御部(105)に送信する。

ステップ809　ファイル制御部(105)が磁気ディスク駆動装置(103)からのデータを受信する。

ステップ810 データの送信が正常に終了すると、磁気ディスク駆動装置(103)は当該読み込み命令の正常終了をファイル制御部(105)に報告する。

ステップ811 ファイル制御部(105)は前記正常終了報告を受信して、当該読み込み命令の正常終了を確認する。

ステップ812　ファイル制御部(105)は、ステップ(811)で受信したデータをクライアント(101)に送信する。

ステップ813 クライアント(101)がファイル制御部(105)が送信するデータを受信する。

ステップ814　データ転送が正常終了すると、ファイル制御部(105)は本読み込み要求が正常終了したことをクライアント(101)に報告する。

ステップ815　クライアント(101)がステップ(814)の正常終了報告を受信して、当該読み込み要求が正常終了したことを確認する。

【００２０】

一般のファイルサーバ装置は、よく利用されるデータをファイル制御部(105)内の半導体メモリに保存して、クライアント(101)に対する応答時間を短くしたり、次に読み込み命令で要求されるデータを予測し、当該データを磁気ディスク駆動装置(103)から読み込み命令に先行して読み込んでおき、応答時間を短くする技術を使用している。図9を使用して、クライアント(101)がファイル制御部(105)に読み込み要求を送信し、要求されたデータがファイル制御部(105)内に保存されていた場合の処理の流れを説明する。時間軸(900)がクライアント(101)の処理の流れを示す。時間軸(901)がファイル制御部(105)の処理の流れを示す。時間軸(902)が磁気ディスク駆動装置(103)の処理の流れを示す。

ステップ903　クライアント(101)がファイル制御部(105)に読み込み要求を送信

する。

ステップ904　ファイル制御部(105)が上記読み込み要求を受信する。

ステップ905　ファイルシステム(115)が受信した情報から、クライアント(101)が要求するデータが磁気ディスク駆動装置(103)のどこに保存されているか探索する。探索の結果、目的のデータがファイル制御部(105)内の半導体メモリに保存されているか判定する。目的のデータがファイル制御部(105)内の半導体メモリに存在しなければ、図8のラダーチャートの処理となる。図9では、目的のデータがファイル制御部(105)内に保存されていた場合を説明する。

ステップ906　ファイル制御部(105)が当該データをクライアント(101)に送信する。

ステップ907　ファイル制御部(105)から送信されるデータをクライアント(101)が受信」する。

ステップ907　データ転送が正常終了すると、ファイル制御部(105)は本読み込み要求が正常終了したことをクライアント(101)に報告する。

ステップ908　クライアント(101)がステップ(907)の正常終了報告を受信して、当該読み込み要求が正常終了したことを確認する。

【００２１】

次に図10を用いてクライアント(101)がデータを書き込む処理を説明する。時間軸(1000)は、クライアント(101)の処理の流れを示す。時間軸(1001)は、ファイル制御部(105)の処理の流れを示す。時間軸(1002)は、磁気ディスク駆動装置(103)の処理の流れを示す。

ステップ1003　クライアント(101)がファイル制御部(105)に対して、ファイルにデータを書き込む要求を送信する。

ステップ1004　ファイル制御部(105)がファイル書き込み要求を受信する。

ステップ1005　クライアント(101)が新しいデータをファイル制御部(105)に送信する。

ステップ1006　ファイル制御部(105)が新しいデータを受信する。

ステップ1007　ファイル制御部(105)は、受信したデータを一旦半導体メモリに保存する。ファイルシステム(115)が受信した情報から、クライアント(101)が要

求するデータが磁気ディスク駆動装置(103)のどこに保存されているか探索する。

ステップ1008　ファイル制御部(105)は、クライアント(101)に書き込み要求が正常に終了したことを報告する。

ステップ1009　クライアント(101)は、ステップ(1008)の報告を受信して、ファイル書き込み要求が正常に終了したことを確認し、次の処理へ移る。

ステップ1010　ファイル制御部(105)は、磁気ディスク駆動装置(103)に書き込み命令を送信する。ステップ(1007)にて当該データが保存されているLUN、LBAは判明しているため、LUN、LBAを送信する。

ステップ1011　磁気ディスク駆動装置(103)がステップ(1010)の書き込み命令を受信する。

ステップ1012　ファイル制御部(105)がデータを磁気ディスク駆動装置(103)に送信する。

ステップ1013　磁気ディスク駆動装置(103)がデータを受信する。

ステップ1014　磁気ディスク駆動装置(103)がデータを正常に受信できたら、ファイル制御部(105)にデータ転送の正常終了を報告する。

ステップ1015　ファイル制御部(105)が正常終了報告を受信して、当該書き込み命令の正常終了を確認する。

【００２２】

図8から10で説明したように、本発明では、データは必ずファイル制御部(105)を経由する。図２に示した従来技術では、データ転送だけはクライアント(101)と磁気ディスク駆動装置(103)間で直接実行される。一見、従来技術の方が効率がよいように見えるが、本発明では以下の点で優れている。

(1)ファイル制御部のキャッシュ効果が期待できる。

(2)クライアントに磁気ディスク駆動装置を直接アクセスする機能が必要ない。

(1)に関しては、図9、10で示したように、ファイル制御部(105)内に目的のデータがあった場合に、ファイル制御部(105)の応答時間が短くなる。クライアント(101)と磁気ディスク駆動装置(103)間で直接データを転送する場合には、このような効果を期待できない。さらに、本発明では、ファイル制御部(105)が利用頻

度の高いデータをファイル制御部(105)内に保存する、あるいは、アクセスパターンを予測し、次にアクセスされる確率の高いデータを、クライアント(101)がアクセスする前に、磁気ディスク駆動装置(103)から読み込んでおくことも可能である。

(2)に関しては、図２に示した従来技術のようにクライアント(101)と磁気ディスク駆動装置(103)間で直接データ転送を行うためには、両者がある1つのプロトコルをサポートする必要がある。したがって、クライアント(101)にそのような機能を実現するソフトウェアなどをインストールする必要がある。一方、本発明では、そのような機能は不要であり、クライアント(101)は一般に普及したNFSやCIFS(Common Internet File System)をサポートしていればよい。

このような点で、ファイル制御部(105)を経由するデータ転送にも優位点がある。

図1の構成のように磁気ディスク駆動装置(103)がファイル制御部(105)だけでなく、クライアント(101)ともLAN(100)あるいはネットワークで接続されている場合には、クライアント(101)が磁気ディスク駆動装置(103)にアクセスすることを制限する必要がある。そのためには、図7の初期化手順に従って、認証情報(109)をクライアント(101)が磁気ディスク駆動装置(103)にアクセスできないようにすることが必要である。以上、説明したように、図1の構成でファイル制御部(105)、磁気ディスク駆動装置(103)が1つのファイルサーバとしてファイルサービスを提供することが可能となる。

<実施例2>

以下、図面を用いてVLAN(Virtual　LAN)技術を用いた本発明のファイルサーバの実現方法を説明する。VLANは、物理的なネットワーク接続とは別に仮想的なネットワークを構築し、構成変更が容易なネットワークシステムを実現する方法である。VLAN技術については、「VPN/VLAN教科書」(是友　春樹監修、マルチメディア通信研究会編、アスキー出版局、1999)に詳しい。LAN(100)は実施例１では、1つの伝送媒体として説明してきたが、物理的には、図11のようにクライアント(101)、磁気ディスク駆動装置(103)、ファイル制御部(105)、管理端末(119)がスイッチングハブ(1100)に結合した形態をとっているのが通例である。VLAN技術

は、スイッチングハブ(1100)にフレームを中継するルールを与えることで仮想的なネットワークを実現する技術である。本実施例では、VLAN技術を用いて図12のような仮想的なネットワークを実現する方法を説明する。すなわち、ファイル制御部(105)と管理端末(119)の間の通信を行う仮想管理LAN(1202)、ファイル制御部(105)とクライアント(101)の間の通信を行う仮想LAN(1200)、ファイル制御部(105)と磁気ディスク駆動装置(103)の間の通信を行う仮想SAN(1201)を実現する。VLAN技術には以下の3種がある。

(1)物理ポートベースVLAN

(2)MACアドレスベースVLAN

(3)プロコトルベースVLAN

がある。(1)の物理ポートベースVLANは、スイッチングハブ(1100)の各物理ポート間で中継ルールを設定することでVLANを実現する。(2)のMACアドレスベースVLANは、ネットワーク上で送受信されるMACフレームに記述される送信元、送信先のMACアドレスに対して中継ルールを設定する方法である。MACアドレスベースVLANは、(1)と比較して柔軟な構成変更が可能である。(3)のプロトコルベースVLANは、MAC層の上位層の種類によってVLANを実現する方法である。本実施例で利用するプロトコルはNFS、iSCSIであるが、これはTCP/IPの上位層プロトコルである。従って、MAC層の上位層プロトコルとしてはTCP/IPを利用している。そのため、仮想管理LAN(1202)、仮想LAN(1200)、仮想SAN(1201)ではTCP/IPを共通に利用しており、プロコトルベースVLANを本実施例に適用することはできない。そこで、本実施例では、MACアドレスベースVLANで説明することにする。MACアドレスベースVLANでは、クライアント(101)、磁気ディスク駆動装置(103)、ファイル制御部(105)、管理端末(119)のMACアドレスをVLANごとに分類する。そしてスイッチングハブ(1100)に対して中継ルールを与える。スイッチングハブ(1100)は、中継するMACフレームの送信元MACアドレスと送信先MACアドレスが同一VLANに属するネットワーク機器のMACアドレスだった場合は当該MACフレームを中継し、異なるVLANに属するネットワーク機器のMACアドレスだった場合には当該MACフレームを中継しない。

【００２３】

このようにしてVLANを実現することができるが、ファイル制御部(105)は複数のVLANに同時に所属することになる。すなわち、ファイル制御部(105)は、仮想管理LAN(1202)と仮想LAN(1200)、仮想SAN(1201)の3つに所属する。通常のネットワーク機器には、1つの物理ポートに1つのMACアドレスが付与される。ファイル制御部(105)は、1つの物理ポートしか持っていない。通常ならば、ファイル制御部(105)は1つのMACアドレスしか持てない。ファイル制御部(105)が1つのMACアドレスしか持てない場合、1つのVLANにしか所属できない。3つのVLANに同時に所属するためには、LAN制御部(114)は、ファイル制御部(105)が所属するVLANの数だけMACアドレスを持つことが必要である。このLAN制御部(114)が本発明の特徴である。

【００２４】

図13を用いて、MACアドレスベースVLANを適用したときのファイル制御部(105)の詳細を説明する。仮想SAN(1201)に対応して、仮想SANMAC層送信キュー(1300)がLAN制御部(114)内に生成される。これは、VLANに対応してMACアドレスが付与されるため、MAC層の送受信キューもVLANに対応して生成される。仮想LAN(1200)に対応して仮想LANMAC層送信キュー(1301)、仮想管理LAN(1202)に対応して仮想管理LANMAC層送信キュー(1302)が生成される。MAC層受信キューについても、同様に仮想SANMAC層受信キュー(1303)、仮想LANMAC層受信キュー(1304)、仮想管理LANMAC層受信キュー(1305)が生成される。これらのMAC層送受信キュー(1300)-(1305)は、上位層送受信キュー(1306)-(1311)と1対1に対応する。さらに、優先度制御部(118)は、優先度設定情報(1312)、転送量管理情報(1313)を持つ。優先度設定情報(1312)は、各仮想チャネルの優先度を保存する。転送量管理情報(1313)は、データ転送量を監視し、各仮想LANごとに、管理者あるいは、優先度制御部(118)が設定した帯域を保存する。

【００２５】

図14を用いて優先度設定情報(1312)を説明する。仮想ネットワーク種別欄(1400)は、仮想ネットワークの種類が設定される。優先度欄(1401)は、仮想ネットワークの優先度が設定される。優先度は管理者が管理端末(119)を操作して設定することができる。優先度欄に設定された数値が大きいほど優先度が高いものとす

る。本実施例では、仮想管理LAN(1202)、仮想LAN(1200)、仮想SAN(1201)を使用するが、それぞれ優先度3、1、2とする。すなわち、仮想管理LAN(1202)の優先度がもっとも高い。仮に仮想管理LAN(1202)の優先度が低い場合、管理者が本ファイルサーバの操作をできなくなることがある。管理者は管理端末(119)を操作し、管理端末(119)は管理者の操作を命令としてファイル制御部(105)に伝える。そのため、仮想管理LAN (1202)の優先度が低いと管理者の操作命令がファイル制御部(105)に遅れて伝達され、この遅延が大きいと事実上ファイルサーバの操作ができなくなる。そのため、仮想管理LAN(1202)の優先度をもっとも高くすべきである。次いで仮想SAN(1201)が優先される。この理由は、以下の通りである。性能を向上させるため、ファイル制御部(105)が磁気ディスク駆動装置(103)のデータをメモリ内にキャッシュする。キャッシュ効果を上げるため、ファイル制御部(105)は、磁気ディスク駆動装置(103)に要求するデータ長は、クライアント(101)がファイル制御部(105)に要求するデータ長よりも大きい。このため、仮想SAN(1201)には仮想LAN(1200)よりも多くの帯域が必要であり、その優先度を高くするのが適切である。

【００２６】

次に図15を用いて転送量管理情報(1313)を説明する。仮想ネットワーク種別欄(1500)は、仮想ネットワークの種類が設定される。転送量欄(1501)は、過去一定時間内に各仮想ネットワーク上で転送したデータサイズの累積値が設定される。優先度制御部(118)は、前記一定時間で転送量欄(1501)の値を0に戻す。設定帯域幅(1502)は、LAN(100)の帯域のうち仮想ネットワークに割り当てる帯域の割合を示す。帯域の絶対値ではなく割合を設定する理由は、データ転送が常に発生しているわけではなく、帯域の絶対値で優先度を評価するのは適切ではないためである。また、帯域幅の割合を設定するのではなく、各々の仮想ネットワークで転送されるデータ量の割合または比率を設定しても本発明を実施することはできるが、ここでは帯域幅の割合を設定するとして以後説明を続ける。優先度欄(1503)は仮想ネットワーク間の優先度が設定される。優先度欄(1503)の優先度は、転送量欄(1501)と設定帯域幅欄(1502)の間の関係から優先度制御部(118)が算出する。例えば、仮想ネットワークに対して番号付けして、仮想ネットワークiの転送量

をX$_i$、設定帯域幅をY$_i$とすると、仮想ネットワークiの利用可能な帯域Δ$_i$は、

【００２７】

【数１】

$$\Delta_i = Y_i - X_i / \sum_{i=1}^{3} X_i \qquad \text{(数式1)}$$

【００２８】

となる。このの大小の順に仮想ネットワークの優先度設定すればよい。すなわち、優先度制御部(118)は、Δ$_i$が大きければ対応する仮想ネットワークの優先度を高くし、Δ$_i$が小さいならば、対応する仮想ネットワークの優先度を低くする。

【００２９】

図１６を用いて、本実施例におけるファイル制御部(105)のデータ受信時の動作を説明する。図16は、優先度制御部(118)が転送量管理情報(1313)を参照して帯域制御を行う場合の動作を示すフローチャートである。

ステップ(1600)　処理の開始。

ステップ(1601)　LAN制御部(114)は転送量管理情報(1313)の優先度欄(1503)を参照し、VLANの処理優先度を確認する。

ステップ(1602)　LAN制御部(114)は、優先度の最も高いMAC層受信キューを参照し、格納されたメッセージを対応する上位層受信キューに移す。

ステップ(1603)　LAN制御部(114)は、対応する上位層の受信処理を実行する。

ステップ(1604)　すべての受信キューのメッセージを処理したか判定する。すべての受信キューの処理が終了していない場合、ステップ(1602)に戻り、次に優先度の高い受信キューに格納されたメッセージに対応する処理を実行する。LAN制御部(114)が、すべての受信キューのメッセージを処理した場合には、ステップ(1605)に進む。

ステップ(1605)　LAN制御(114)は、ステップ(1604)で受信したデータサイズの累計を上位層の受信キュー(1509)、(1510)、(1511)ごとに計算する。

ステップ(1606)　LAN制御部(114)は、ステップ(1605)で計算した受信データサイズの累計を仮想ネットワークごとに転送量欄(1501)に加算する。

ステップ(1607)　優先度制御部(118)は、ステップ(1606)で更新された転送量欄

(1501)の数値から、(数式1)によって計算した優先度を優先度欄(1503)に仮想ネットワークごとに設定する。

ステップ(1608)　処理の終了。

【００３０】

図17を用いて、本実施例におけるLAN制御部(114)のデータ送信時の動作を説明する。図17は、LAN制御部(114)が転送量管理情報(1313)を参照して帯域制御を行う場合の動作を示すフローチャートである。

ステップ(1700)　処理の開始。

ステップ(1701)　LAN制御部(114)は転送量管理情報(1313)の優先度欄(1503)を参照し、優先度を確認する。

ステップ(1702)　LAN制御部(114)は、優先度の最も高い上位層送信キューを参照し、格納されたメッセージを対応するMAC層送信キューに移す。

ステップ(1703)　LAN制御部(114)は、対応するMAC層の送信処理を実行する。

ステップ(1704)　LAN制御部(114)は、すべての送信キューのメッセージを処理したか判定する。すべての送信キューの処理が終了していない場合、ステップ(1702)に戻り、次に優先度の高い送信キュー処理を実行する。LAN制御部(114)が、すべての受信キューのメッセージを処理した場合には、ステップ(1705)に進む。

ステップ(1705)　LAN制御部(114)は、ステップ(1703)で送信したデータサイズの累計を上位層の送信キュー(1306)、(1307)、(1308)ごとに計算する。

ステップ(1706)　LAN制御部(114)は、ステップ(1705)で計算した送信データサイズの累計を仮想ネットワークごとに転送量欄(1501)に加算する。

ステップ(1707)　優先度制御部(118)は、ステップ(1706)で更新された転送量欄(1501)の数値から、(数式1)によって計算した優先度を優先度欄(1503)に仮想ネットワークごとに設定する。

ステップ(1708)　処理の終了。

【００３１】

次に、優先度設定情報(1312)を用いて、あらかじめ設定された優先度に従ってLAN制御部(114)が送受信制御を行う処理を説明する。図18を用いて、本実施例におけるLAN制御部(114)のデータ受信時の動作を説明する。

ステップ(1800)　処理の開始。

ステップ(1801)　LAN制御部(114)は転送量管理情報(1313)の優先度欄(1503)を参照し、優先度を確認する。

ステップ(1802)　LAN制御部(114)は、優先度の最も高いMAC層受信キューを参照し、格納されたメッセージを対応する上位層受信キューに移す。

ステップ(1803)　LAN制御部(114)は、対応する上位層の受信処理を実行する。

ステップ(1804)　LAN制御部(114)は、すべての受信キューのメッセージを処理したか判定する。すべての受信キューの処理が終了していない場合、ステップ(1802)に戻り、次に優先度の高い受信キュー処理を実行する。LAN制御部(118)が、すべての受信キューのメッセージを処理した場合には、ステップ(1805)に進む。

ステップ(1805)　処理の終了。

【００３２】

図19を用いて、本実施例におけるLAN制御部(114)のデータ送信時の動作を説明する

ステップ(1900)　処理の開始。

ステップ(1901)　LAN制御部(114)は転送量管理情報(1313)の優先度欄(1503)を参照し、優先度を確認する。

ステップ(1902)　LAN制御部(114)は、優先度の最も高い上位層送信キューを参照し、格納されたメッセージを対応するMAC層送信キューに移す。

ステップ(1903)　LAN制御部(114)は、対応するMAC層の送信処理を実行する。

ステップ(1904)　LAN制御部(114)は、すべての送信キューのメッセージを処理したか判定する。すべての送信キューの処理が終了していない場合、ステップ(1902)に戻り、次に優先度の高い送信キュー処理を実行する。LAN制御部(114)が、すべての受信キューのメッセージを処理した場合には、ステップ(1905)に進む。

ステップ(1905)　処理の終了。

以上、説明したように、あらかじめ設定された優先度に従ってLAN制御部(114)がLAN(100)上の仮想ネットワークの通信の優先制御を行うことができる。また、予め各仮想ネットワークごとに設定された帯域幅に従ってLAN制御部(114)は通信の帯域制御を行うことができる。このような優先制御、帯域制御は、スイッチ、ル

ータなどの通信を中継する機器ではよく知られた技術であるが、ファイル制御部(105)のような通信を発信、受信する機器(エンドポイントという)でこのような制御を行うことによって、利用目的に応じた仮想ネットワーク間の優先制御、帯域制御が可能になるという効果を発揮できる。

【００３３】

また、ここで説明した仮想ネットワークにおける優先制御、帯域制御は、例えば非特許文献２で開示されている暗号化を用いる場合のようなVLAN以外の手段で構築された仮想ネットワークにも適応できる。

【００３４】

<実施例３>

図25を用いて、LAN(100)に複数の磁気ディスク駆動装置を内蔵した磁気ディスク装置が接続したシステムにおける本発明の適用例を説明する。磁気ディスク装置(2500)は、磁気ディスク制御装置(2501)と磁気ディスク駆動装置(2502)がファイバチャネルSAN(2504)を介して結合した構成をとる。磁気ディスク駆動装置(2502)は、磁気ディスク媒体(2505)、ディスク制御部(2506)からなる。ディスク制御部(2506)はこれまで説明した実施例1-3で紹介した磁気ディスク制御部(107)と異なり、ファイバチャネルインタフェースを持つ。ファイバチャネルSAN(2504)は、閉じたネットワークであるため、磁気ディスク制御部(107)には存在した、認証機能などのセキュリティ機能は必要ない。本発明によれば、ファイル制御部(105)と磁気ディスク装置(2500)の間に仮想ネットワークを確立させることにより、データの保護、帯域制御を実現することができる。したがって、実施例1-3では磁気ディスク駆動装置(103)に必要だった認証制御部(108)、認証情報(109)を磁気ディスク制御装置(2501)が持つことになる。したがって、磁気ディスク制御装置(2501)が持つ認証制御部(2509)、認証情報(2510)は、実施例1で説明した認証制御部(108)、認証情報(109)と同様の機能をもつものである。

【００３５】

図25の磁気ディスク装置(2500)は、ファイル制御部(105)に対してサービスを提供する単位として仮想ディスクという単位を用いることがある。仮想ディスクとは、磁気ディスク制御装置(2501)が磁気ディスク駆動装置(2502)の記憶領域の

一部またはすべてを、ファイル制御部(105)に対して1つの磁気ディスク駆動装置として認識させた場合におけるこの仮想的な磁気ディスク駆動装置のことをいう。仮想ディスクは磁気ディスク駆動装置(2501)が仮想的に実現したものであり、複数の磁気ディスク駆動装置を1つの仮想ディスクとして実現するなど、さまざまな実現例がある。この仮想ディスクは、ファイル制御部(105)からは物理的な実体である磁気ディスク駆動装置(2502)とは区別できない。この仮想ディスクを図26に示す。ファイル制御部(105)からみれば、LAN(100)に仮想ディスク(2600)、(2601)、(2602)が接続しているように見えるだけで、磁気ディスク制御装置(2501)などは認識できない。本発明によれば、図27に示すように、仮想LAN(1200)、仮想SAN(1201)、仮想管理LAN(1202)を生成することができる。仮想ディスク(2600)、(2601)、(2602)は、仮想SAN(1201)に接続され、クライアント(101)、管理端末(119)はこれら仮想ディスク(2600)、(2601)、(2602)にアクセスできない。

【００３６】

さらに、図27の変形例として、ファイル制御部(105)が仮想ディスク(2600)、(2601)、(2602)ごとにセキュリティ設定を行う方式も考えられる。その場合、認証情報(2510)は、図4で示した認証情報(109)の形式と異なってくる。この場合の認証情報(2510)の形式を図28に示す。仮想ディスク識別子(2800)は、磁気ディスク制御装置(2501)が仮想ディスク(2600)、(2601)、(2602)に付与した識別子である。MACアドレス欄(2801)は、図4のMACアドレス欄(400)と同様に、アクセスを許すネットワーク機器のMACアドレスを磁気ディスク制御装置(2501)が設定する欄である。IPアドレス欄(2802)は、図4のIPアドレス欄(401)と同様に、アクセスを許すネットワーク機器のIPアドレスを磁気ディスク制御装置(2501)が設定する欄である。認証コード(2803)は、図4の認証コード欄(402)と同様に、アクセスを許すネットワーク機器の認証コードを磁気ディスク制御装置(2501)が設定する欄である。オーナフラグ欄(2804)は、図4のオーナフラグ欄(400)と同様に、MACアドレス欄(2801)に設定されたネットワーク機器がこの仮想ディスクのオーナ権限を持っているかどうかを示す欄である。このように、内蔵する仮想ディスク(2600)、(2601)、(2602)ごとにセキュリティ設定を可能とすることで、仮想ディスクの一部は、ファイル制御部(105)の管理下におくが、その他の仮想ディスクはクラ

イアント(101)の管理下におくという使用方法が可能となる。

【００３７】

<実施例４>

図29を用いて本発明第4の実施例を説明する。図29において、実施例1と比較して、ネットワークのトポロジが異なっている。クライアント(101)と管理端末(119)は、一般LAN(2900)に結合しており、一般LAN(2900)はファイアウォール(2901)を介して、ファイル制御部(105)と結合している。磁気ディスク駆動装置(103)は、LAN(100)と結合しているが、一般LAN(2900)と同様にファイアウォール(2901)を介して、ファイル制御部(105)と結合している。ファイアウォールのアクセス制御部(2902)は、クライアント(101)、ファイル制御部(105)、磁気ディスク駆動装置(103)、管理端末(119)間の通信を制御する。すなわち、ファイアウォールのアクセス制御部(2902)は、クライアント(101)、管理端末(119)のファイル制御部(105)との通信データは中継するが、磁気ディスク駆動装置(103)との通信データは中継しない制御を行う。また、ファイアウォールのアクセス制御部(2902)は、磁気ディスク駆動装置(103)のファイル制御部(105)間の通信データは中継するが、それ以外の通信データは中継しない。このような制御を行うことにより、磁気ディスク駆動装置(103)のデータがファイル制御部(105)以外のネットワーク機器から参照、改変されることを防ぐことができる。

【００３８】

また、ファイアウォール(2901)のアクセス制御は、ユーザの設定が必要になるが、管理端末(119)、クライアント(101)から設定可能であっては、意味がない。管理端末(119)、クライアント(101)がファイアウォール(2901)のアクセス制御方針を変更して、磁気ディスク駆動装置(103)に直接アクセスすることが可能になるからである。従って、ファイアウォール(2901)のアクセス制御に関する設定は、ファイアウォール(2901)に物理的に結合したコンソール(2903)のみが変更可能とするべきである。あるいは、ファイル制御部(105)がファイアウォール(2901)のアクセス制御情報を変更する手段をもつということも考えられるが、物理的に直接結合した経路(2904)経由でしか変更を許さない方が望ましい。

【００３９】

【発明の効果】

本発明のファイルサーバは、磁気ディスク駆動装置がファイル制御部以外の機器と通信することを制限する手段を持っているため、クライアントが直接磁気ディスク駆動装置にアクセスして、データを破壊、漏洩することを防ぐことができる。

【００４０】

さらに、本発明では、VLAN技術等の仮想ネットワークをファイルサーバに適用するため、クライアント、管理端末が磁気ディスク駆動装置に直接アクセスすることを禁止できる。

【００４１】

また、前述の仮想ネットワークの別の効果としては、管理端末、クライアント、磁気ディスク駆動装置を異なる仮想ネットワークに所属させることで、管理端末がファイル制御部とクライアントの間の通信を観測することを防ぐことが可能となる効果がある。

【００４２】

そして、本発明のファイルサーバでは、ファイル制御部がLAN通信処理の優先度を、通信相手ごとに設定することを許容するため、管理端末との通信を最優先に処理するように設定でき、管理端末からファイルサーバを常に操作可能となる。また本発明の方法は、ファイル制御部が過大なネットワーク負荷をかける攻撃を受けた場合でも、管理端末から操作可能であり、ファイルサービスが停止しないという効果もある。

【００４３】

また、本発明の二次的効果として、データは必ずファイル制御部を経由するため、クライアントと磁気ディスク駆動装置の間で直接データ転送を行うための特殊な機能をクライアント、磁気ディスク駆動装置に搭載することが不要になる。

【図面の簡単な説明】

【図１】

本発明のファイルサーバの構成図である。

【図２】

従来技術のファイルサーバの構成図である。

【図３】

構成情報(117)の内容を示した表図である。

【図４】

認証情報(109)の初期状態を示した表図である。

【図５】

認証情報(109)の初期化完了後の状態を示した表図である。

【図６】

磁気ディスク駆動装置(103)の認証情報設定処理のフローチャートである。

【図７】

ファイル制御部（105）と磁気ディスク駆動装置（103）の初期化の過程を示したラダーチャートである。

【図８】

本発明のファイル制御部(105)に対してクライアント(101)がファイル読み込み要求を送信した場合の動作を示すラダーチャートである。

【図９】

本発明のファイル制御部(105)に対してクライアント(101)がファイル読み込み要求を送信し、目的のデータがファイル制御部(105)内に存在した場合の動作を示すラダーチャートである。

【図１０】

本発明のファイル制御部(105)に対してクライアント(101)がファイル書き込み要求を送信した場合の動作を示すラダーチャートである。

【図１１】

本発明の第2の実施例の構成図である。

【図１２】

図１１において、仮想ネットワークを生成したときの、概念図である。

【図１３】

本発明のファイル制御部(105)において、仮想ネットワークによる通信を行ったときの内部状態を示す図である。

【図１４】

優先度設定情報(1312)を示す表図である。

【図１５】

転送量管理情報(1313)を示す表図である。

【図１６】

帯域制御を行った場合のファイル制御部(105)の受信処理を示したフローチャートである。

【図１７】

帯域制御を行った場合のファイル制御部(105)の送信処理を示したフローチャートである。

【図１８】

優先度設定を行った場合のファイル制御部(105)の受信処理を示したフローチャートである。

【図１９】

優先度設定を行った場合のファイル制御部(105)の送信処理を示したフローチャートである。

【図２０】

VLAN技術でなく、暗号化により仮想ネットワークを生成したときの、ファイル制御部(105)の内部状態を示した図である。

【図２１】

優先度設定を行った場合のファイル制御部(105)の受信処理を示したフローチャートである。

【図２２】

優先度設定を行った場合のファイル制御部(105)の送信処理を示したフローチャートである。

【図２３】

帯域制御を行った場合のファイル制御部(105)の受信処理を示したフローチャートである。

【図２４】

帯域制御を行った場合のファイル制御部（105）の送信処理を示したフローチャートである。

【図２５】

LAN(100)に磁気ディスク装置(2500)が接続されたときの構成図である。

【図２６】

ファイル制御部(105)が認識する仮想ディスクとの接続形態を示す概念図である。

【図２７】

図２５のシステムに本発明の仮想ネットワークを適用したときの概念図である。

【図２８】

認証情報(2510)の内容を示す表図である。

【図２９】

本発明の第4の実施例の構成図である。

【符号の説明】

100.　LAN

101.　クライアント

103.　磁気ディスク駆動装置

105.　ファイル制御部

106.　磁気ディスク媒体

107.　磁気ディスク制御部

108.　認証制御部

109.　認証情報

110.　磁気ディスク媒体

114.　LANコントローラ

115.　　ファイルシステム

116.　アクセス制御部

117.　構成情報

118.　優先度制御部

119.　管理端末

300.　番号

301.　MACアドレス欄

302.　IPアドレス欄

303.　HDD識別子欄

304.　Alias名欄

305.　磁気ディスク駆動装置に関する情報のエントリ

306.　磁気ディスク駆動装置に関する情報のエントリ

307.　磁気ディスク駆動装置に関する情報のエントリ

308.　磁気ディスク駆動装置に関する情報のエントリ

400.　MACアドレス欄

401.　IPアドレス欄

402.　認証コード欄

403.　オーナフラグ欄

404.　MACアドレスのエントリ

405.　IPアドレスのエントリ

406.　認証コードのエントリ

407.　オーナフラグのエントリ

500.　MACアドレス欄

501.　IPアドレス欄

502.　認証コード欄

503.　オーナフラグ欄

504.　MACアドレスのエントリ

505.　IPアドレスのエントリ

506.　認証コードのエントリ

507.　オーナフラグのエントリ

600.　電源投入ステップ

601.　認証情報の変更命令を受信したか判定するステップ

602.　オーナフラグが「1」のエントリがあるか判定するステップ

603.　当該変更命令は所有者が発行したものか判定するステップ
604.　認証情報を変更するステップ
605.　認証情報の変更をファイル制御部に報告するステップ
606.　認証情報の変更に失敗したことを報告するステップ
607.　認証情報を設定するステップ
608.　オーナフラグを設定するステップ
609.　処理の終了
700.　ファイル制御部の処理の流れ
701.　磁気ディスク駆動装置の処理の流れ
702.　ファイル制御部の電源投入ステップ
703.　次期ディスク駆動装置の電源投入ステップ
704.　ファイル制御部の制御ソフトが起動するステップ
705.　磁気ディスク駆動装置がネットワーク設定を行うステップ
706.　ディスカバリメッセージ送信ステップ
707.　ディスカバリメッセージ受信ステップ
708.　ディスカバリメッセージへの応答を送信するステップ
709.　ディスカバリメッセージへの応答を受信するステップ
710.　磁気ディスク駆動装置の起動を確認するステップ
711.　認証情報設定メッセージを送信するステップ
712.　認証情報設定メッセージを送信するステップ
713.　認証情報を変更するステップ
714.　認証情報の変更が完了したことを報告するステップ
715.　認証情報変更完了報告メッセージを受信するステップ
716.　ログインメッセージ送信ステップ
717.　ログインメッセージ受信ステップ
718.　認証情報を確認するステップ
719.　ログイン受諾メッセージ送信ステップ
720.　ログイン受諾メッセージ受信ステップ
721.　磁気ディスク駆動装置へのアクセスを開始するステップ

800.　クライアントの処理の流れ
801.　ファイル制御部の処理の流れ
802.　磁気ディスク駆動装置の処理の流れ
803.　ファイルリード要求送信ステップ
804.　ファイルリード要求受信ステップ
805.　ファイルシステム処理ステップ
806.　ディスク読み込み命令発行ステップ
807.　ディスク読み込み命令受信ステップ
808.　データ送信ステップ
809.　データ受信ステップ
810.　送信完了報告ステップ
811.　ディスク読み込み命令終了確認ステップ
812.　データ送信ステップ
813.　データ受信ステップ
814.　送信完了報告ステップ
815.　ファイル読み込み処理終了確認ステップ
900.　クライアント処理の流れ
901.　ファイル制御部の処理の流れ
902.　磁気ディスク駆動装置の処理の流れ
903.　ファイルリード要求発行ステップ
904.　ファイルリード要求受信ステップ
905.　ファイルシステム処理ステップ
906.　データ送信ステップ
907.　データ受信ステップ
908.　送信完了報告ステップ
909.　ファイル読み込み処理終了確認ステップ
1000.　クライアントの処理の流れ
1001.　ファイル制御部の処理の流れ
1002.　磁気ディスク駆動装置の処理の流れ

1003.　ファイルライト要求発行ステップ
1004.　ファイルライト要求受信ステップ
1005.　データ送信ステップ
1006.　データ受信ステップ
1007.　ファイルシステム処理ステップ
1008.　受信完了報告ステップ
1009.　ファイル書き込み完了ステップ
1010.　ディスク書き込み命令発行ステップ
1011.　ディスク書き込み命令受信ステップ
1012.　データ送信ステップ
1013.　データ受信ステップ
1014.　受信完了報告ステップ
1015.　ディスク書き込み完了ステップ
1100.　スイッチングハブ
1200.　仮想LAN
1201.　仮想SAN
1202.　仮想管理LAN
1300.　仮想SANMAC層送信キュー
1301.　仮想LANMAC層送信キュー
1302.　仮想管理LANMAC層送信キュー
1303.　仮想SANMAC層受信キュー
1304.　仮想LANMAC層受信キュー
1305.　仮想管理LANMAC層受信キュー
1306.　仮想SAN送信キュー
1307.　仮想LAN送信キュー
1308.　仮想管理LAN送信キュー
1309.　仮想SAN受信キュー
1310.　仮想LAN受信キュー
1311.　仮想管理LAN受信キュー

1400.　仮想ネットワーク種別欄

1401.　優先度欄

1402.　仮想管理LANのエントリ

1403.　仮想LANのエントリ

1404.　仮想SANのエントリ

1500.　仮想ネットワーク欄

1501.　転送量欄

1502.　設定帯域幅

1503.　優先度欄

1504.　仮想管理LANのエントリ

1505.　仮想LANのエントリ

1600.　処理の開始

1601.　転送量管理情報を参照するステップ

1602.　MAC層受信キューを参照するステップ

1603.　上位層処理を実行するキュー

1604.　すべてのキューの受信処理が終了したか判定するステップ

1605.　データ転送量を仮想ネットワークごとに計算するステップ

1606.　転送量管理情報を変更するステップ

1607.　優先度を変更するステップ

1608.　処理の終了

1700.　処理の開始

1701.　転送量管理情報を参照するステップ

1702.　上位層送信キューを参照するステップ

1703.　MAC層処理を実行するステップ

1704.　すべてのキューの送信処理が終了したか判定するステップ

1705.　データ転送量を仮想ネットワークごとに計算するステップ

1706.　転送量管理情報を変更するステップ

1707.　優先度を変更するステップ

1708.　処理の終了

1800.　処理の開始

1801.　優先度設定情報を参照するステップ

1802.　MAC層受信キューを参照するステップ

1803.　上位層処理を実行するキュー

1804.　すべてのキューの受信処理が終了したか判定するステップ

1805.　処理の終了

1900.　処理の開始

1901.　優先度設定情報を参照するステップ

1902.　上位層送信キューを参照するステップ

1903.　MAC層処理を実行するキュー

1904.　すべてのキューの送信処理が終了したか判定するステップ

1905.　処理の終了

2000.　MAC層送信キュー

2001.　MAC層受信キュー

2100.　処理の開始

2101.　MAC受信キューを参照するステップ

2102.　メッセージを上位層キューに振り分けるステップ

2103.　上位層処理ステップ

2104.　処理の終了

2200.　処理の開始

2201.　上位層送信キューを参照するステップ

2202.　メッセージをMAC層送信キューに挿入するステップ

2203.　MAC層処理ステップ

2204.　処理の終了

2300.　処理の開始

2301.　上位層送信キューを参照するステップ

2302.　優先度に従って上位層キューのメッセージをMAC層送信キューに挿入するステップ

2303.　MAC層送信キューに挿入された順序に送信処理を実行するステップ

2304.　データ転送量を上位層キューごとに計算するステップ

2305.　転送量管理情報を変更するステップ

2306.　優先度を変更

2307.　処理の終了

2400.　処理の開始

2401.　MAC層受信キューを参照するステップ

2402.　MAC層受信キューのメッセージを上位層キューに振り分けるステップ

2403.　指定された優先度で上位層キューの処理を実行するステップ

2404.　データ転送量を上位層キューごとに計算するステップ

2405.　転送量管理情報を変更するステップ

2406.　優先度を変更

2407.　処理の終了

2500.　磁気ディスク装置

2501.　磁気ディスク制御装置

2502.　磁気ディスク駆動装置

2504.　ファイバチャネルSAN

2505.　磁気ディスク媒体

2506.　ディスク制御部

2509.　認証制御部

2510.　認証情報

2600.　仮想ディスク

2601.　仮想ディスク

2602.　仮想ディスク2800.　仮想ディスク識別子欄

2801.　MACアドレス欄

2802.　IPアドレス欄

2803.　認証コード欄

2804.　オーナフラグ欄

2805.　仮想ディスク(2600)のエントリ

2806.　仮想ディスク(2601)のエントリ

2900.　一般LAN

2901.　ファイアウォール

2902.　アクセス制御部

2903.　コンソール

2904.　ファイル制御部(105)とファイアウォール(2901)との通信路。

【書類名】　　図面

【図１】

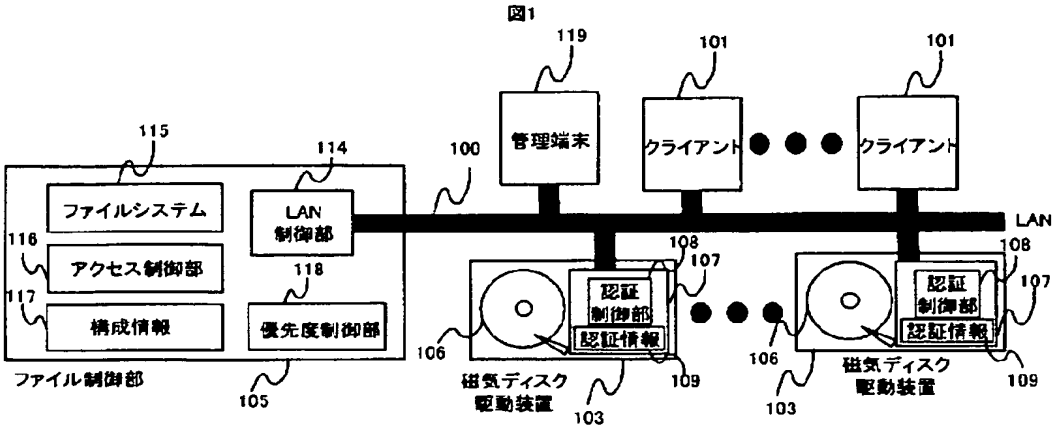


図1
119
101
101
管理端末
クライアント
クライアント
115
114
100
ファイルシステム
LAN
制御部
LAN
116
アクセス制御部
108
107
108
107
118
117
構成情報
優先度制御部
認証
制御部
認証
制御部
106
認証情報
106
認証情報
ファイル制御部
105
磁気ディスク
駆動装置
109
磁気ディスク
駆動装置
109
103
103

【図２】

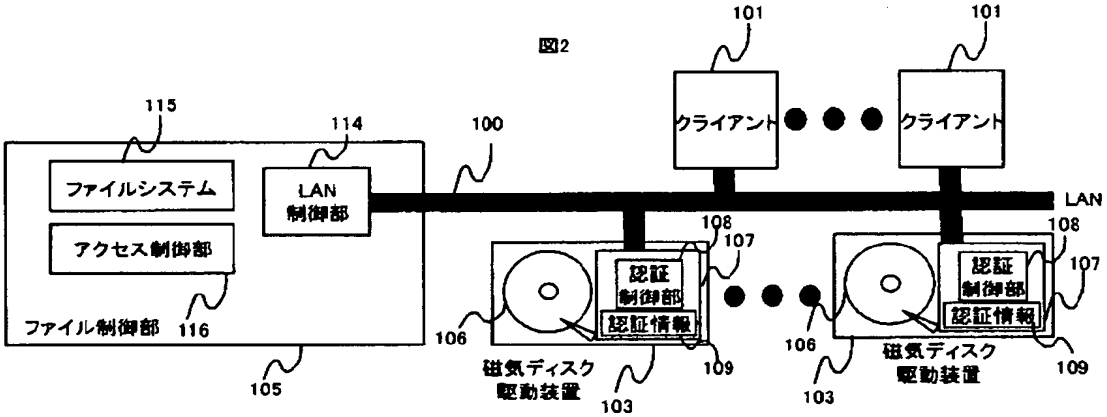
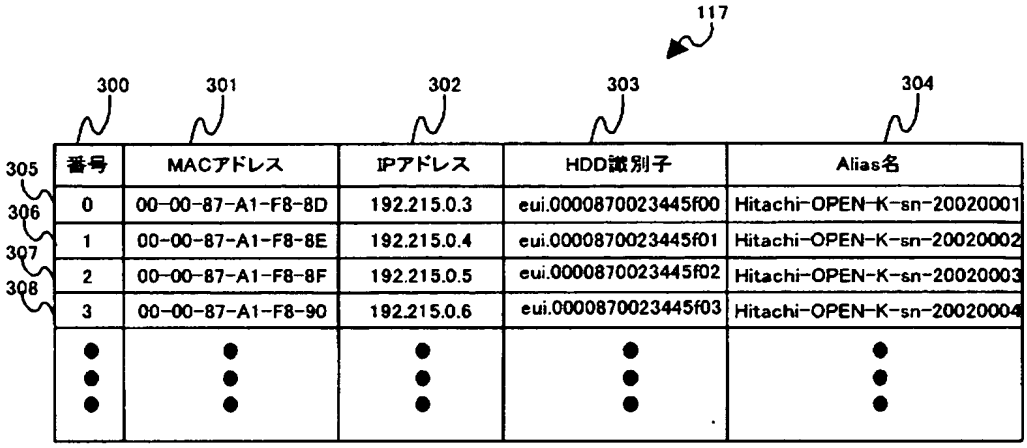


図2
101
101
クライアント
クライアント
115
114
100
ファイルシステム
LAN
制御部
LAN
アクセス制御部
108
107
108
107
認証
制御部
認証
制御部
106
認証情報
106
認証情報
ファイル制御部
116
105
磁気ディスク
駆動装置
109
磁気ディスク
駆動装置
109
103
103

【図３】

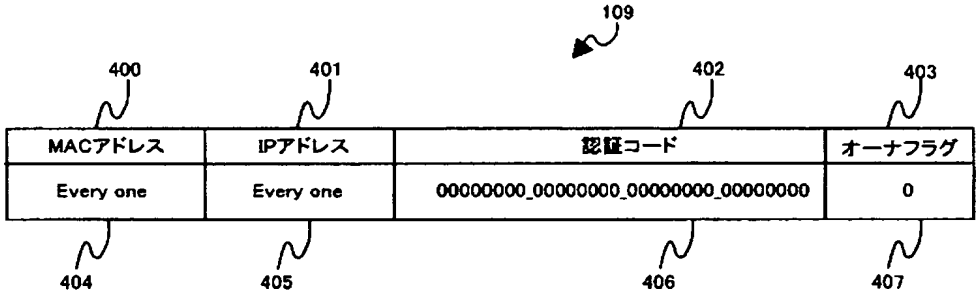
図3



番号	MACアドレス	IPアドレス	HDD識別子	Alias名
0	00-00-87-A1-F8-8D	192.215.0.3	eui.0000870023445f00	Hitachi-OPEN-K-sn-20020001
1	00-00-87-A1-F8-8E	192.215.0.4	eui.0000870023445f01	Hitachi-OPEN-K-sn-20020002
2	00-00-87-A1-F8-8F	192.215.0.5	eui.0000870023445f02	Hitachi-OPEN-K-sn-20020003
3	00-00-87-A1-F8-90	192.215.0.6	eui.0000870023445f03	Hitachi-OPEN-K-sn-20020004
●	●	●	●	●
●	●	●	●	●
●	●	●	●	●

【図４】

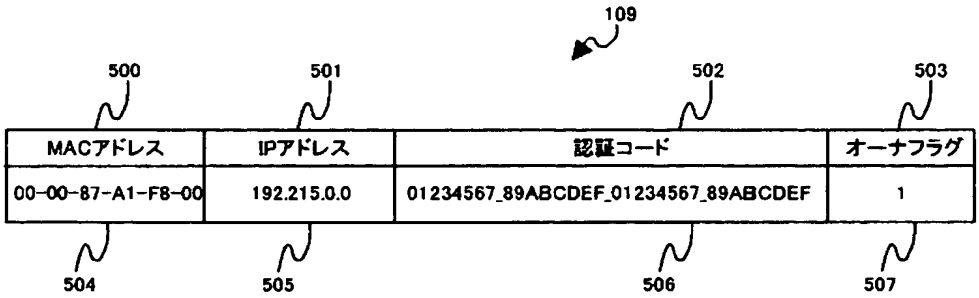
図4



MACアドレス	IPアドレス	認証コード	オーナフラグ
Every one	Every one	00000000_00000000_00000000_00000000	0

【図５】

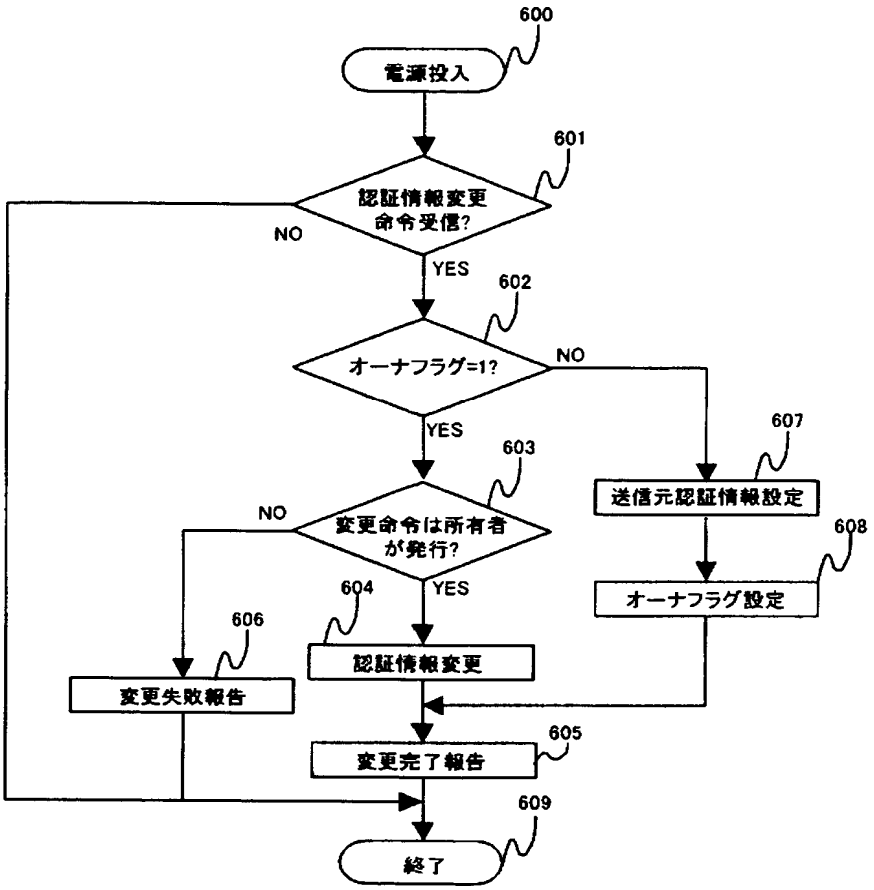
図5



MACアドレス	IPアドレス	認証コード	オーナフラグ
00-00-87-A1-F8-00	192.215.0.0	01234567_89ABCDEF_01234567_89ABCDEF	1

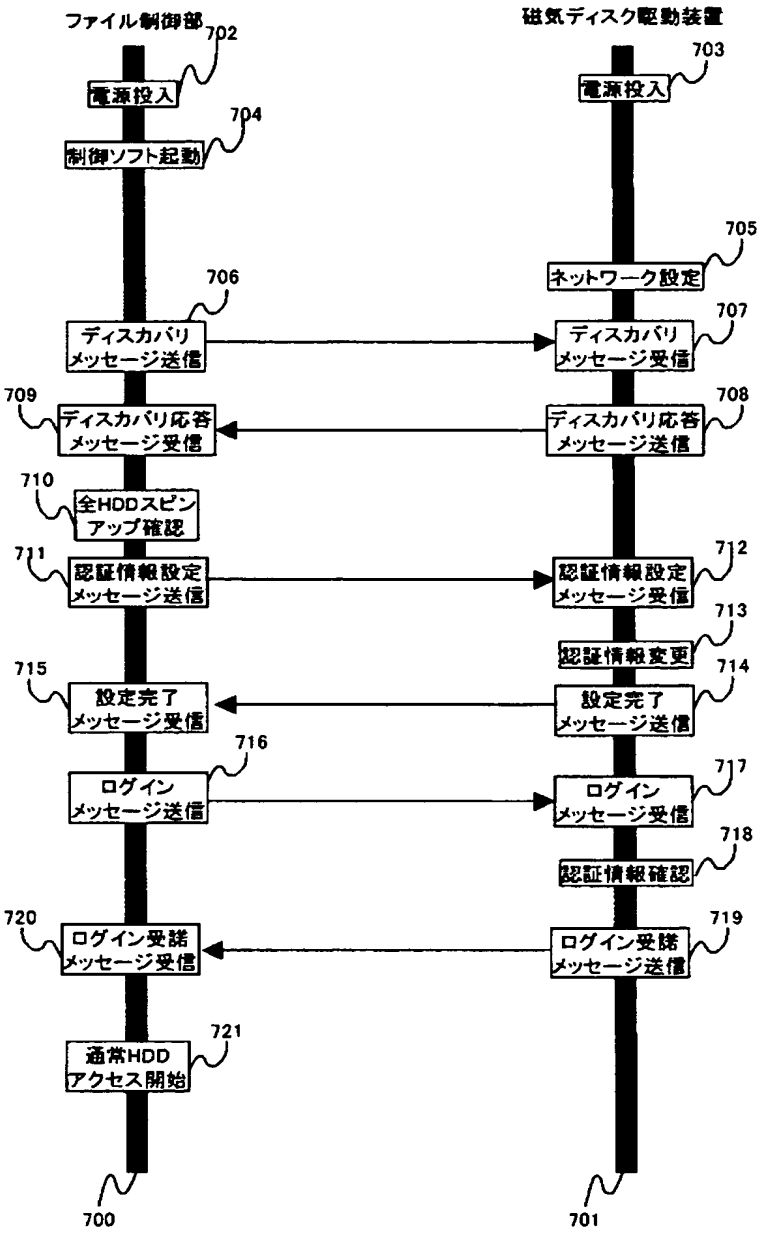
【図６】

図6


600
電源投入
601
認証情報変更
命令受信?
NO
YES
602
オーナフラグ=1?
NO
YES
603
変更命令は所有者
が発行?
NO
YES
604
認証情報変更
606
変更失敗報告
605
変更完了報告
607
送信元認証情報設定
608
オーナフラグ設定
609
終了

【図７】

図7


ファイル制御部
磁気ディスク駆動装置
702
703
電源投入
電源投入
704
制御ソフト起動
705
ネットワーク設定
706
707
ディスカバリ
メッセージ送信
ディスカバリ
メッセージ受信
709
708
ディスカバリ応答
メッセージ受信
ディスカバリ応答
メッセージ送信
710
全HDDスピン
アップ確認
711
712
認証情報設定
メッセージ送信
認証情報設定
メッセージ受信
713
認証情報変更
715
714
設定完了
メッセージ受信
設定完了
メッセージ送信
716
717
ログイン
メッセージ送信
ログイン
メッセージ受信
718
認証情報確認
720
719
ログイン受諾
メッセージ受信
ログイン受諾
メッセージ送信
721
通常HDD
アクセス開始
700
701

【図８】

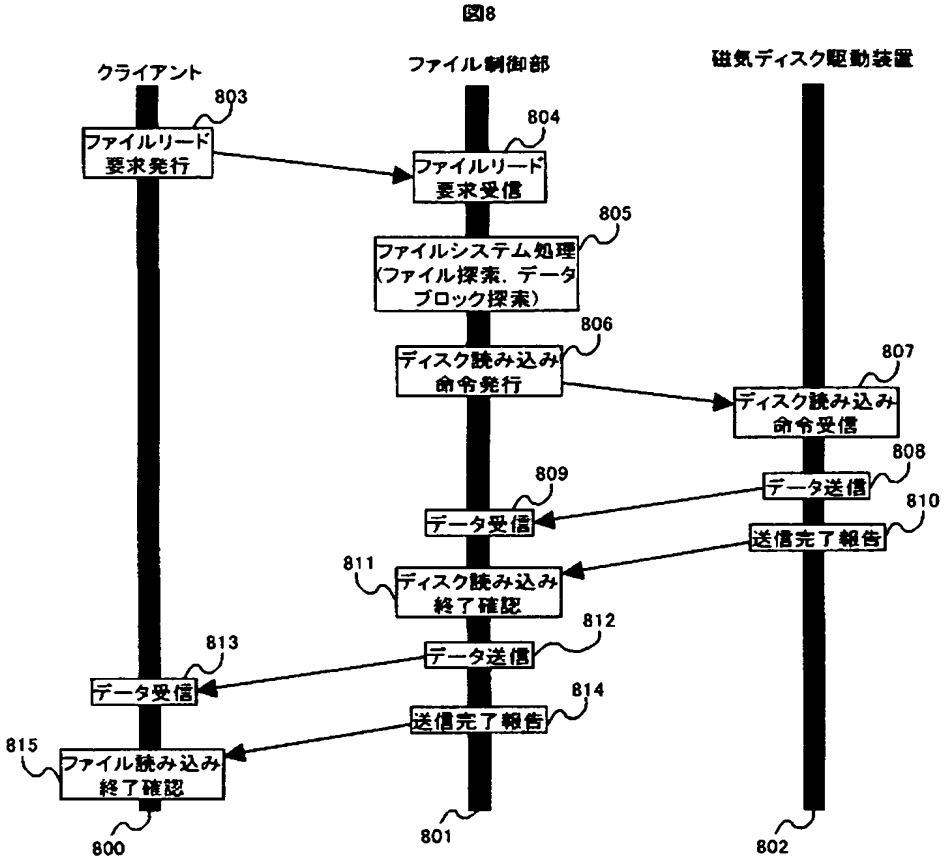


図8
クライアント
ファイル制御部
磁気ディスク駆動装置
803
ファイルリード要求発行
804
ファイルリード要求受信
805
ファイルシステム処理(ファイル探索，データブロック探索)
806
ディスク読み込み命令発行
807
ディスク読み込み命令受信
808
データ送信
809
データ受信
810
送信完了報告
811
ディスク読み込み終了確認
812
データ送信
813
データ受信
814
送信完了報告
815
ファイル読み込み終了確認
800
801
802

【図９】

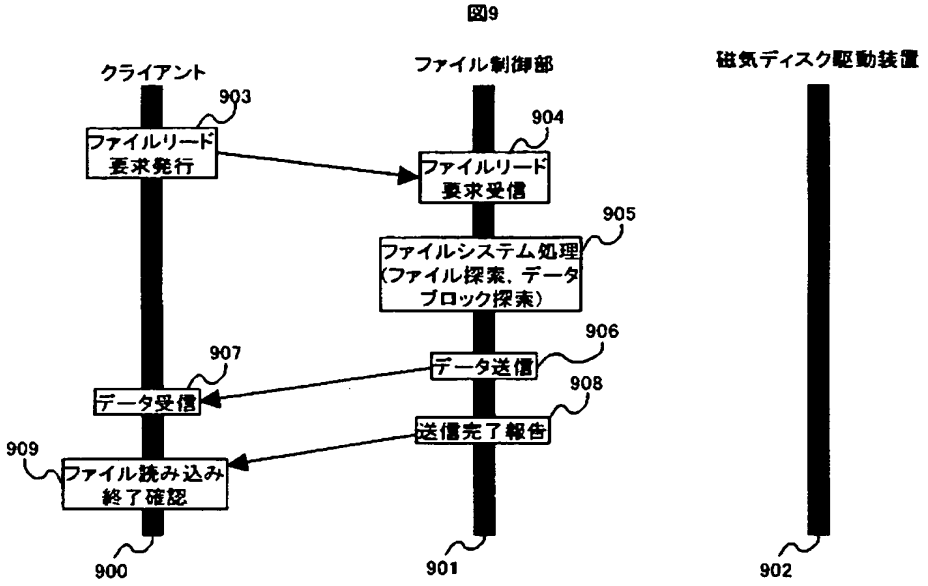


図9
クライアント
ファイル制御部
磁気ディスク駆動装置
903
ファイルリード
要求発行
904
ファイルリード
要求受信
905
ファイルシステム処理
(ファイル探索，データ
ブロック探索)
906
データ送信
907
データ受信
908
送信完了報告
909
ファイル読み込み
終了確認
900
901
902

【図１０】

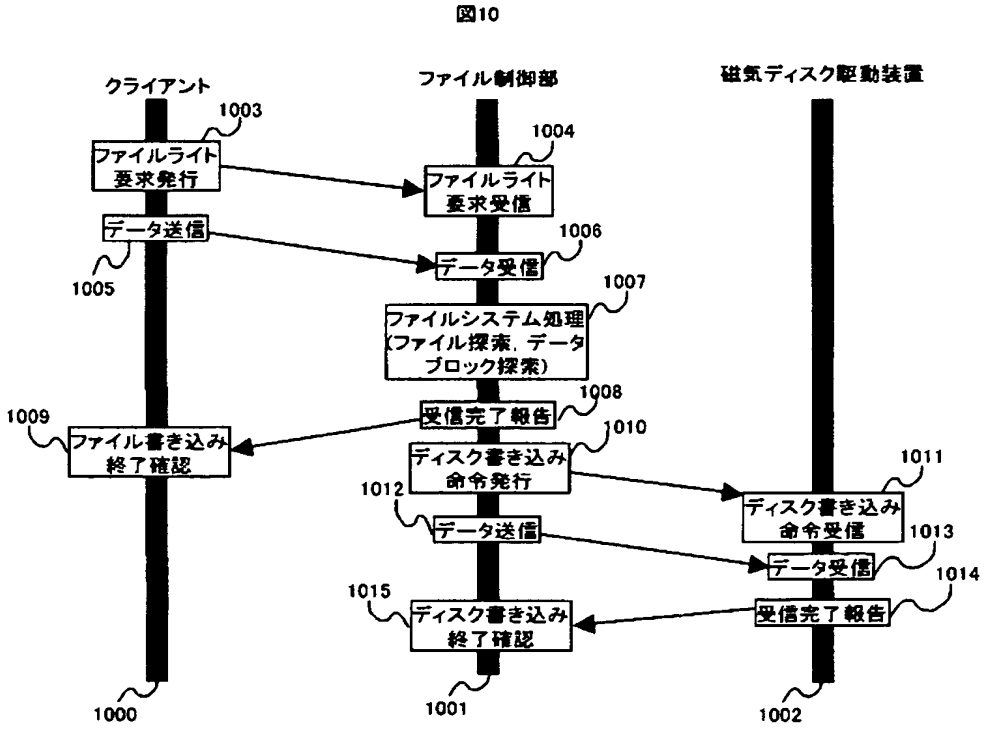
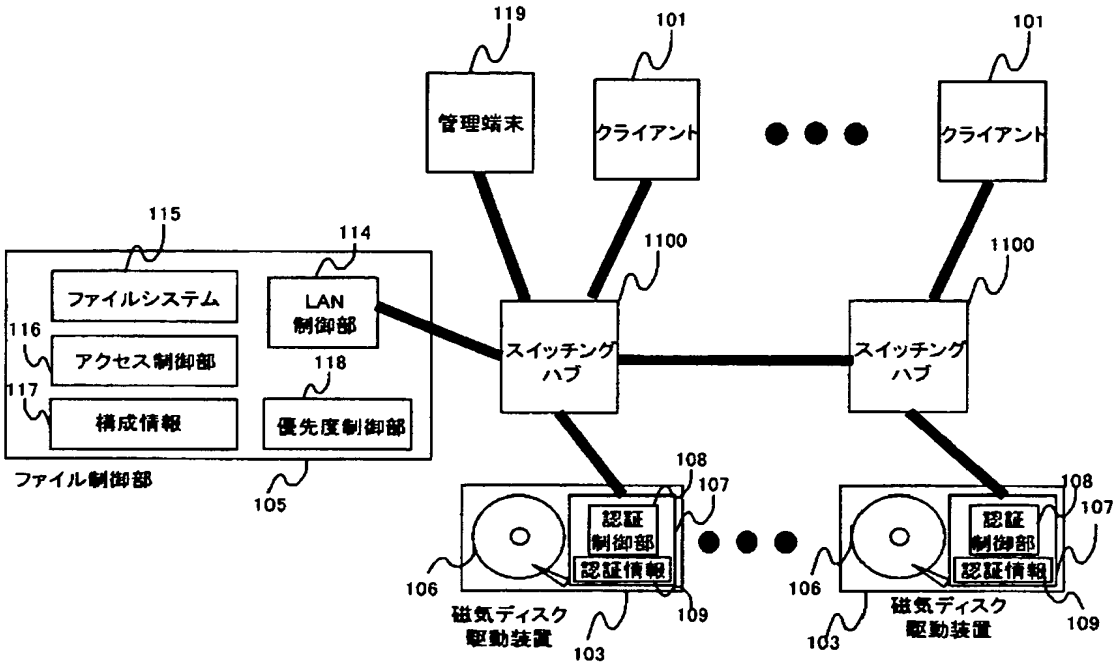


図10
クライアント
ファイル制御部
磁気ディスク駆動装置
1003
ファイルライト
要求発行
1004
ファイルライト
要求受信
データ送信
1005
1006
データ受信
1007
ファイルシステム処理
(ファイル探索，データ
ブロック探索)
1008
受信完了報告
1009
ファイル書き込み
終了確認
1010
ディスク書き込み
命令発行
1011
ディスク書き込み
命令受信
1012
データ送信
1013
データ受信
1014
受信完了報告
1015
ディスク書き込み
終了確認
1000
1001
1002

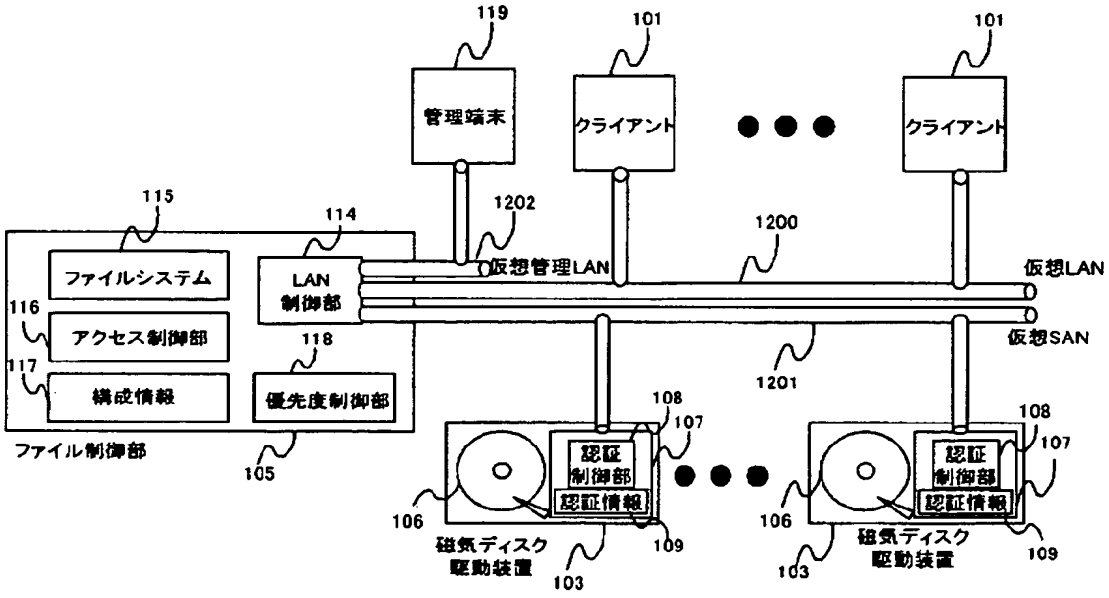
【図１１】

図11

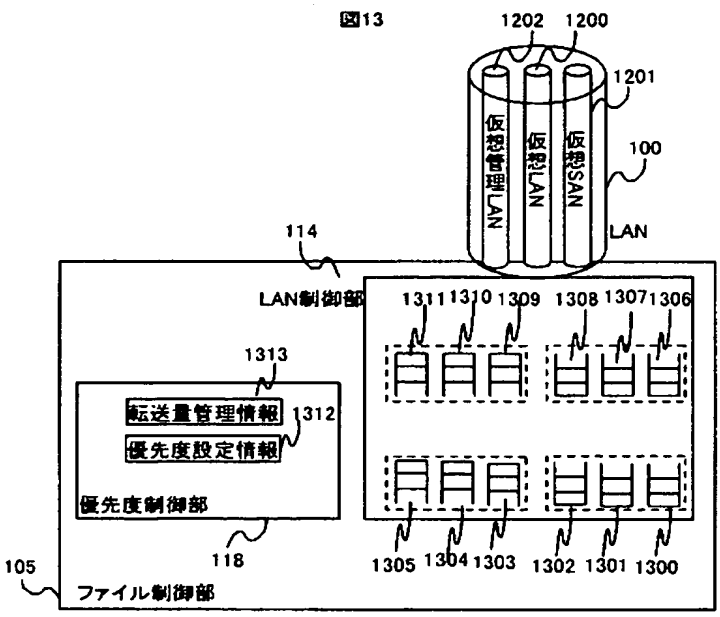


【図１２】

図12



【図１３】



【図１４】

図14

1312

1400 仮想ネットワーク種別	1401 優先度
仮想管理LAN	3
仮想LAN	1
仮想SAN	2

【図１５】

図15

1313

1500 仮想ネットワーク	1501 転送量	1502 設定帯域幅	1503 優先度
仮想管理LAN	51	10%	3
仮想LAN	64123543	40%	1
仮想SAN	556498333	50%	2

【図１６】

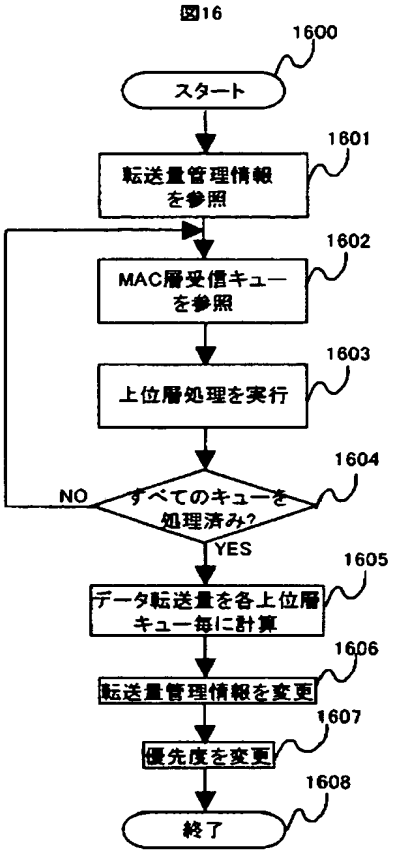


図16
1600
スタート
1601
転送量管理情報を参照
1602
MAC層受信キューを参照
1603
上位層処理を実行
1604
すべてのキューを処理済み?
NO
YES
1605
データ転送量を各上位層キュー毎に計算
1606
転送量管理情報を変更
1607
優先度を変更
1608
終了

【図１７】

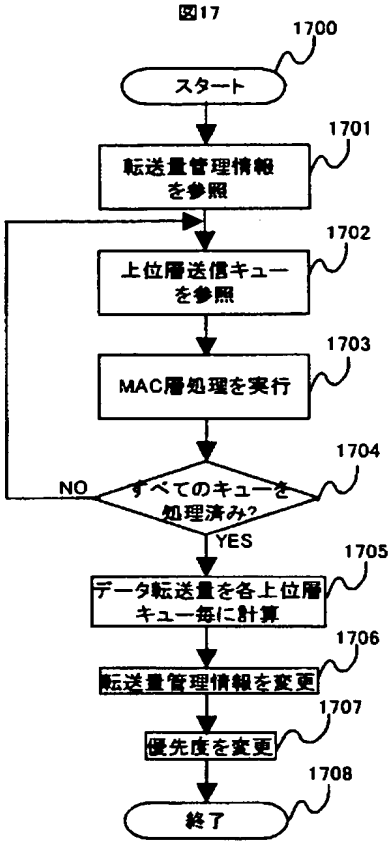


図17
1700
スタート
1701
転送量管理情報を参照
1702
上位層送信キューを参照
1703
MAC層処理を実行
1704
すべてのキューを処理済み?
NO
YES
1705
データ転送量を各上位層キュー毎に計算
1706
転送量管理情報を変更
1707
優先度を変更
1708
終了

【図１８】

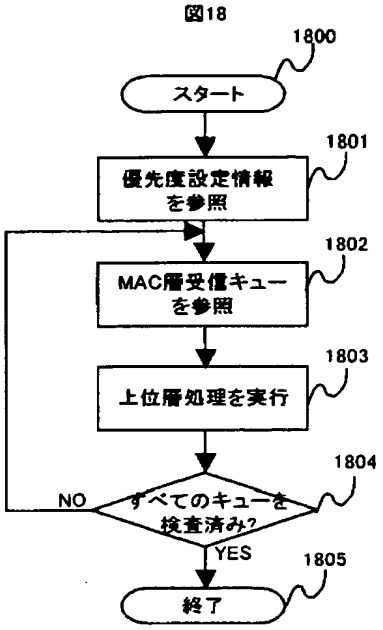


図18
1800
スタート
1801
優先度設定情報を参照
1802
MAC層受信キューを参照
1803
上位層処理を実行
1804
NO
すべてのキューを検査済み?
YES
1805
終了

【図１９】

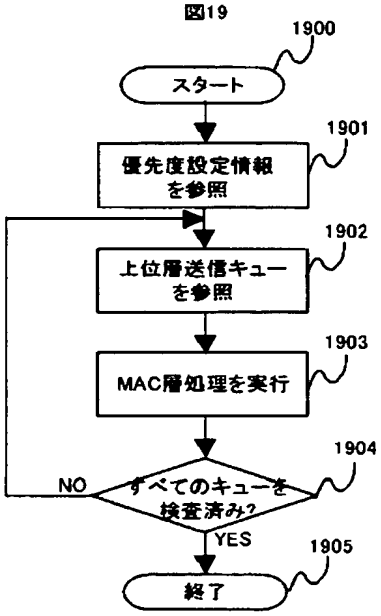


図19
1900
スタート
1901
優先度設定情報を参照
1902
上位層送信キューを参照
1903
MAC層処理を実行
1904
NO
すべてのキューを検査済み?
YES
1905
終了

【図２０】

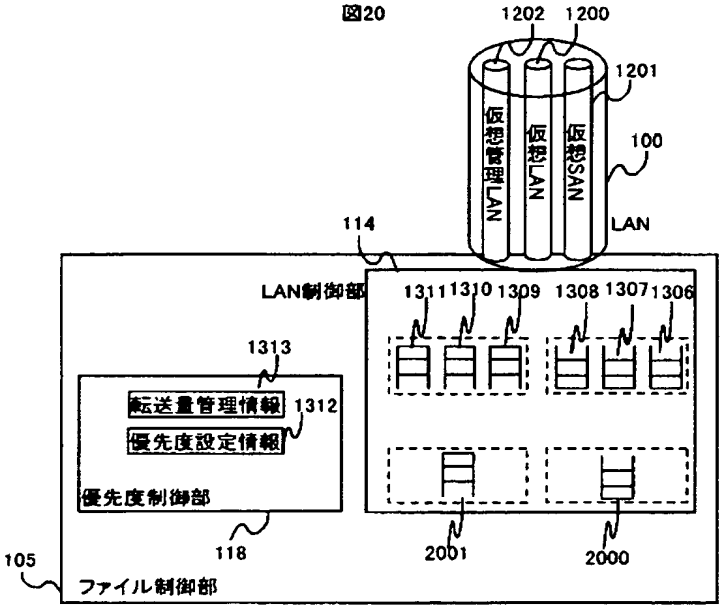


図20
1202
1200
1201
仮想管理LAN
仮想LAN
仮想SAN
100
LAN
114
LAN制御部
1311
1310
1309
1308
1307
1306
1313
転送量管理情報
1312
優先度設定情報
優先度制御部
118
2001
2000
105
ファイル制御部

【図２１】

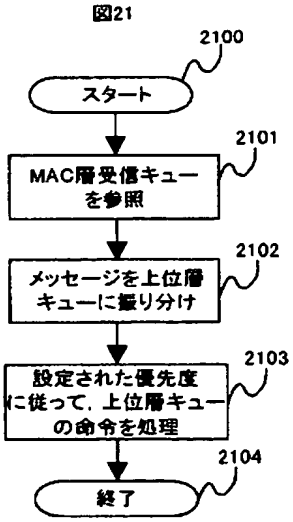


図21
2100
スタート
2101
MAC層受信キューを参照
2102
メッセージを上位層キューに振り分け
2103
設定された優先度に従って，上位層キューの命令を処理
2104
終了

【図２２】

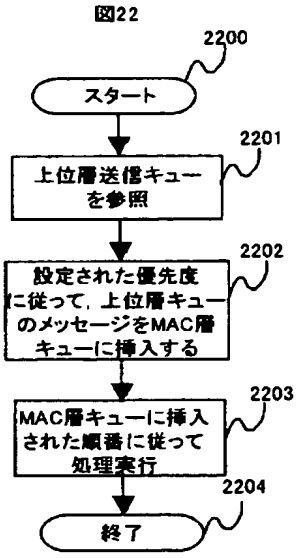


図22
2200
スタート
2201
上位層送信キューを参照
2202
設定された優先度に従って，上位層キューのメッセージをMAC層キューに挿入する
2203
MAC層キューに挿入された順番に従って処理実行
2204
終了

【図２３】

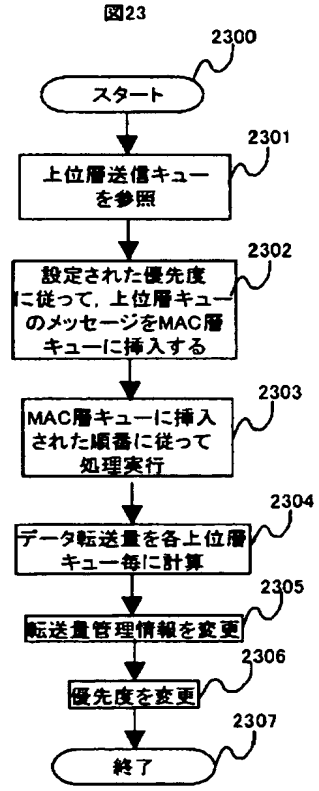
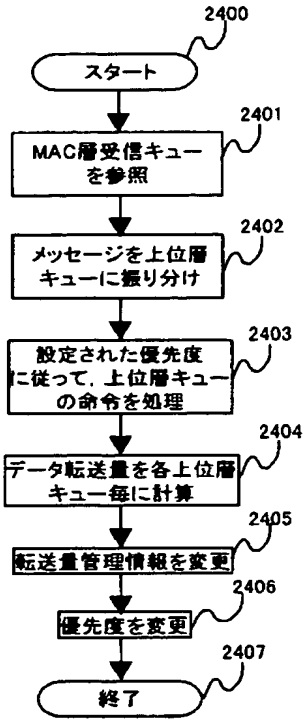


図23
2300
スタート
2301
上位層送信キューを参照
2302
設定された優先度に従って，上位層キューのメッセージをMAC層キューに挿入する
2303
MAC層キューに挿入された順番に従って処理実行
2304
データ転送量を各上位層キュー毎に計算
2305
転送量管理情報を変更
2306
優先度を変更
2307
終了

【図２４】

図24


2400
スタート
2401
MAC層受信キューを参照
2402
メッセージを上位層キューに振り分け
2403
設定された優先度に従って，上位層キューの命令を処理
2404
データ転送量を各上位層キュー毎に計算
2405
転送量管理情報を変更
2406
優先度を変更
2407
終了

【図２５】

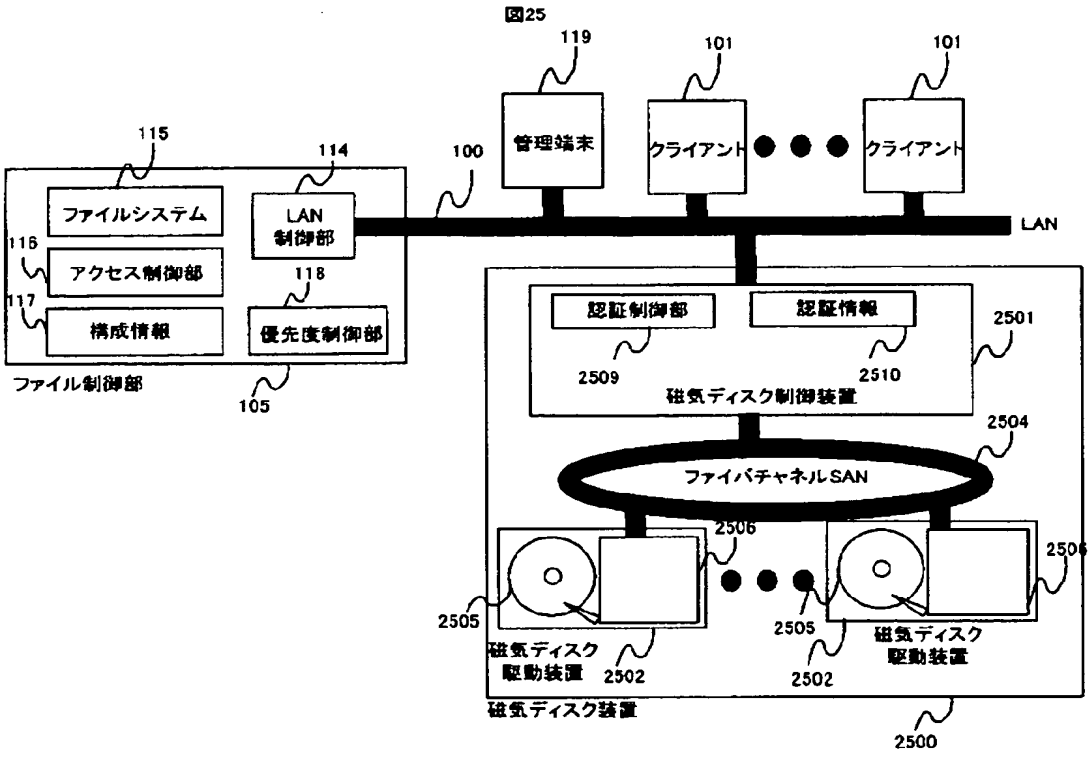


図25
119
101
101
管理端末
クライアント
クライアント
115
114
100
ファイルシステム
LAN
制御部
LAN
116
アクセス制御部
118
117
構成情報
優先度制御部
ファイル制御部
105
認証制御部
認証情報
2501
2509
2510
磁気ディスク制御装置
2504
ファイバチャネルSAN
2506
2506
2505
2505
磁気ディスク
駆動装置
2502
2502
磁気ディスク
駆動装置
磁気ディスク装置
2500

【図２６】

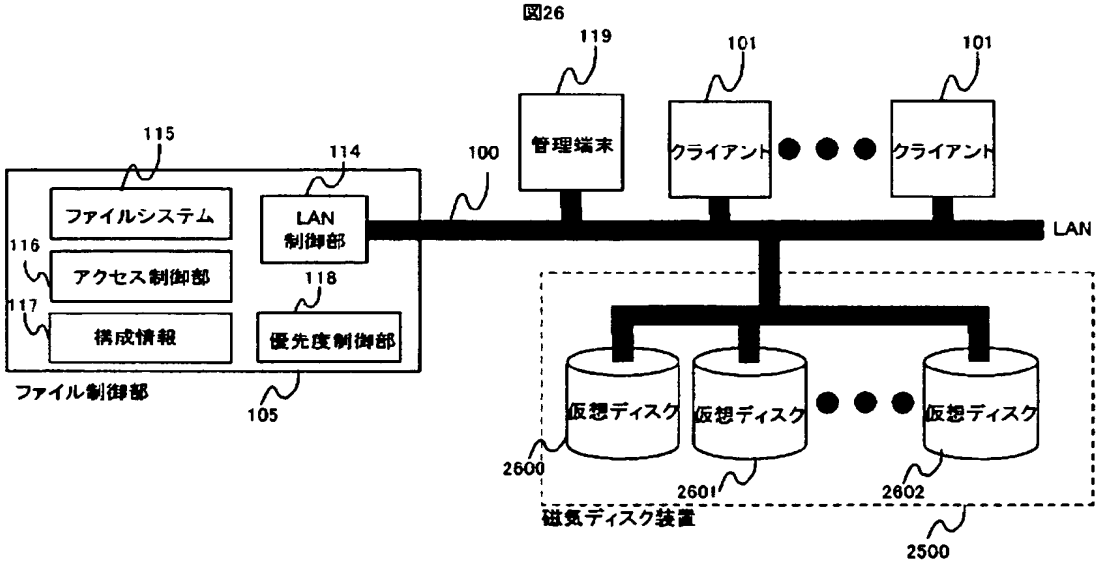
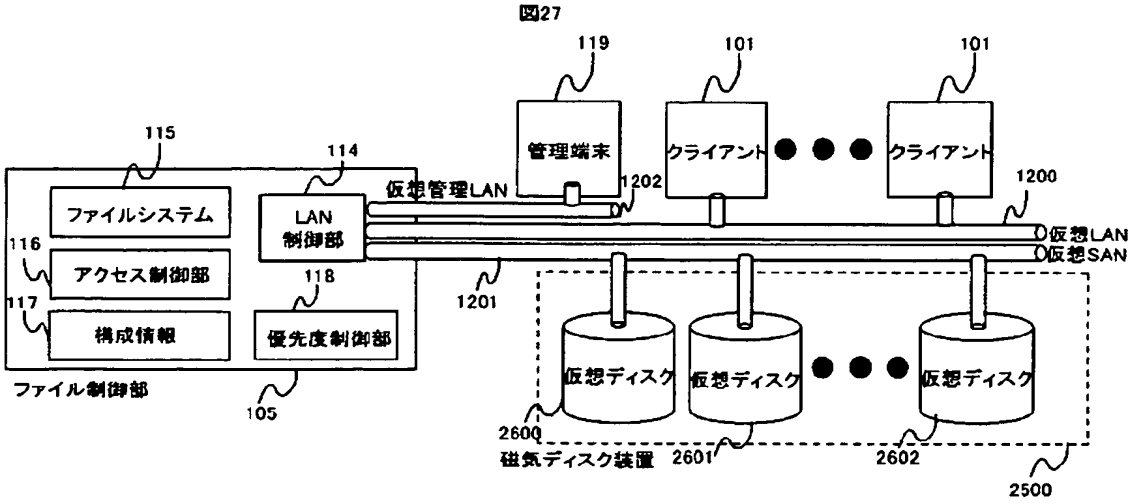


図26
119
101
101
管理端末
クライアント
クライアント
115
114
100
ファイルシステム
LAN
制御部
LAN
116
アクセス制御部
118
117
構成情報
優先度制御部
ファイル制御部
105
仮想ディスク
仮想ディスク
仮想ディスク
2600
2601
2602
磁気ディスク装置
2500

【図２７】

図27



【図２８】

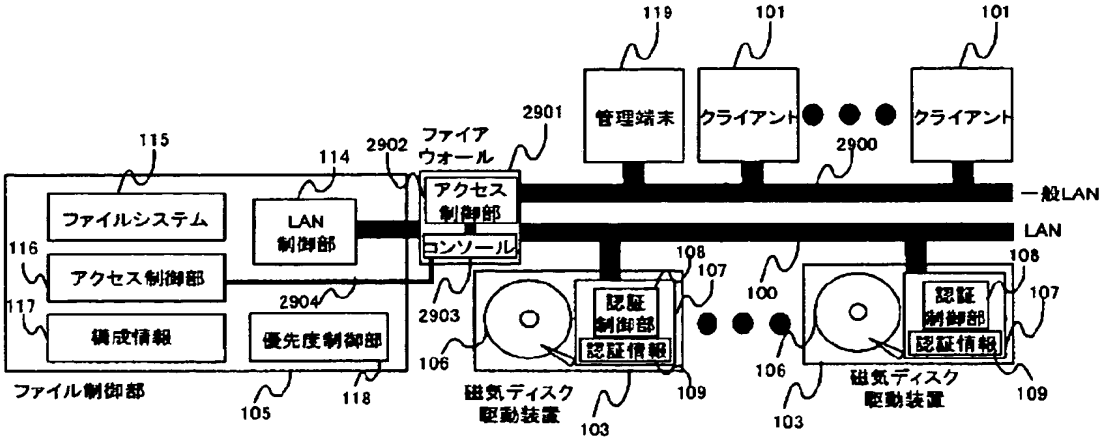
図28

2510

2800	2801	2802	2803	2804	2805
仮想ディスク識別子	MACアドレス	IPアドレス	認証コード	オーナフラグ	
2600	Every one	Every one	00000000_00000000_00000000_00000000	0	2806
2601	Every one	Every one	00000000_00000000_00000000_00000000	0	
●	●	●	●	●	

【図２９】

図29


119
101
101
管理端末
クライアント
クライアント
2901
2902
ファイア
ウォール
2900
115
114
アクセス
制御部
一般LAN
ファイルシステム
LAN
制御部
コンソール
LAN
116
アクセス制御部
108
107
108
107
2904
2903
100
117
構成情報
優先度制御部
認証
制御部
認証
制御部
106
106
認証情報
認証情報
109
109
ファイル制御部
磁気ディスク
駆動装置
磁気ディスク
駆動装置
105
118
103
103

【書類名】　　要約書

【要約】

【課題】　LAN直結型磁気ディスク駆動装置を使ってファイルサーバを構成すると、他のネットワーク機器から磁気ディスク駆動装置をアクセスできるという問題があった。

【解決手段】　ファイル制御部が磁気ディスク駆動装置の起動時に、他のネットワーク機器からのアクセスを禁止できる手段を設ける。

【効果】　磁気ディスク駆動装置にアクセスできるネットワーク機器がファイル制御部のみとなり、データの安全性が高まる。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－１５６１２７
受付番号	５０３００９１２１２７
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　６月　３日

＜認定情報・付加情報＞

【提出日】　平成15年 6月 2日

次頁無

特願２００３－１５６１２７

出　願　人　履　歴　情　報

識別番号　　［０００００５１０８］

１．変更年月日　　１９９０年　８月３１日
［変更理由］　　新規登録
住　所　　東京都千代田区神田駿河台４丁目６番地
氏　名　　株式会社日立製作所